UNIVERSIDADE ESTADUAL DO MARANHÃO
CENTRO DE CIÊNCIAS SOCIAIS APLICADAS
CURSO DE DIREITO BACHARELADO

DANIEL VITOR REZENDE CAMPOS

A RESPONSABILIDADE CIVIL DO ESTADO POR VAZAMENTOS DE DADOS SIGILOSOS DE BANCO DE DADOS DO CNJ A PARTIR DA LEI GERAL DE PROTEÇÃO DE DADOS

Bacabal
2026

DANIEL VITOR REZENDE CAMPOS

A RESPONSABILIDADE CIVIL DO ESTADO POR VAZAMENTOS DE DADOS SIGILOSOS DE BANCO DE DADOS DO CNJ A PARTIR DA LEI GERAL DE PROTEÇÃO DE DADOS

Trabalho de Conclusão de Curso apresentado ao Curso de Direito Bacharelado da Universidade Estadual do Maranhão – UEMA, *campus* Bacabal, como requisito para obtenção do grau de Bacharel em Direito.

Orientadora: Prof.ª. Esp. Keila da Silva Ferreira Castro

Bacabal
2026

Campos, Daniel Vitor Rezende.

A responsabilidade civil do Estado por vazamentos de dados sigilosos de banco de dados do CNJ a partir da Lei Geral de Proteção de Dados / Daniel Vitor Rezende Campos. - Bacabal - MA, 2026.

71 f.

Monografia (Graduação em Direito Bacharelado) - Universidade Estadual do Maranhão, Campus Bacabal, 2026.

Orientadora: Profa. Esp. Keila da Silva Ferreira Castro.

1. responsabilidade civil do Estado. 2. Proteção de dados pessoais. 3. Lei Geral de Proteção de Dados. 4. Conselho Nacional de Justiça. 5. Bancos de dados. I. Título.

CDU: 342.721(81)

Elaborado por Anderson de Araújo Machado - CRB 13/746

DANIEL VITOR REZENDE CAMPOS

A RESPONSABILIDADE CIVIL DO ESTADO POR VAZAMENTOS DE DADOS SIGILOSOS DE BANCO DE DADOS DO CNJ A PARTIR DA LEI GERAL DE PROTEÇÃO DE DADOS

Trabalho de Conclusão de Curso apresentado ao Curso de Direito Bacharelado da Universidade Estadual do Maranhão – UEMA, *campus* Bacabal, como requisito para obtenção do grau de Bacharel em Direito.

Orientador: Prof.ª. Esp. Keila da Silva Ferreira Castro

Aprovada em: _____/____/_____

BANCA EXAMINADORA

KEILA DA SILVA FERREIRA CASTRO:04026785327

Assinado de forma digital por KEILA DA SILVA FERREIRA CASTRO:04026785327
Dados: 2026.07.29 11:10:01 -03'00'

Orientadora: Prof.ª. Esp. Keila da Silva Ferreira Castro
Especialista em Direito Constitucional
Universidade Estadual do Maranhão – UEMA

gov.br Documento assinado digitalmente
MEIRELENE PEREIRA FROES LIMA
Data: 29/07/2026 16:10:40-0300
Verifique em https://validar.iti.gov.br

1° Examinador (a):
Universidade Estadual do Maranhão – UEMA

gov.br Documento assinado digitalmente
PEDRO HENRIQUE GONCALVES CLEMENTINO
Data: 29/07/2026 17:29:29-0300
Verifique em https://validar.iti.gov.br

2° Examinador (a):
Universidade Estadual do Maranhão – UEMA

Dedico este trabalho a Deus, pela sua eterna misericórdia e à minha família, os verdadeiros responsáveis por esta realização.

AGRADECIMENTOS

Primeiro, agradeço a Deus por ser a expressão máxima de misericórdia, segurança e refúgio nos momentos difíceis.

Agradeço à minha família, em especial à minha mãe, Marilene Nascimento de Rezende pelo amor, apoio, pela paciência e pela confiança depositada em mim, por nunca ter desistido e por sempre ter sido minha inspiração. Agradeço à minha vó, Maria Concebida Nascimento de Rezende pelos cuidados, pela sabedoria e pelo carinho que muito estimo. Agradeço à minha irmã, Daniela Fernanda Nascimento de Rezende, por ser minha amiga, pelos conselhos, pela confiança, por ser determinante para as minhas convicções.

Aos meus amigos, por terem me acompanhado e por resistirem as minhas ladainhas infinitas, agradeço pelo incentivo, pela escuta e pelos momentos de apoio, especialmente nos períodos de grande cansaço e insegurança.

Aos professores da UEMA que fizeram parte da minha formação acadêmica, deixo meu reconhecimento pelos ensinamentos transmitidos durante o curso e pela contribuição para o meu desenvolvimento pessoal e profissional.

De modo especial, meus mais sinceros agradecimentos à Prof. Keila da Silva Ferreira Castro, pela orientação recebida na elaboração deste trabalho, pela atenção, pelas sugestões, especialmente pela sua paciência e pelo auxílio na conclusão desta etapa, que certamente seria excessivamente mais onerosa sem sua intervenção.

A todos que, direta ou indiretamente, contribuíram para a realização desta etapa, deixo meu agradecimento.

RESUMO

A presente monografia analisa a responsabilidade civil do Estado diante de incidentes de segurança envolvendo dados pessoais administrados pelo Conselho Nacional de Justiça. Parte-se do exame da evolução histórica da responsabilidade estatal, desde a superação da teoria da irresponsabilidade até a consolidação da responsabilidade objetiva fundada no risco administrativo, prevista no artigo 37, § 6º, da Constituição Federal de 1988. Em seguida, investiga-se a proteção jurídica da privacidade e dos dados pessoais no ordenamento brasileiro, considerando sua relação com a dignidade da pessoa humana, os direitos da personalidade, a autodeterminação informativa e a disciplina estabelecida pela Lei Geral de Proteção de Dados Pessoais. O estudo demonstra que o CNJ, ao coordenar e administrar bases nacionais do Poder Judiciário, atua como controlador de dados pessoais e se submete aos deveres de segurança, prevenção e governança previstos na LGPD e em suas próprias normas institucionais. A concentração de informações processuais, criminais, familiares, patrimoniais e sensíveis amplia os riscos decorrentes de acessos indevidos e vazamentos, exigindo proteção compatível com a relevância dos dados tratados. Conclui-se que a responsabilização civil do Estado, nesses casos, não decorre automaticamente da simples ocorrência do incidente, mas depende da verificação dos pressupostos jurídicos do dever de indenizar, especialmente a existência de dano, o nexo causal e a falha no cumprimento dos deveres legais de proteção.

Palavras-chave: responsabilidade civil do Estado; proteção de dados pessoais; Lei Geral de Proteção de Dados; Conselho Nacional de Justiça; bancos de dados.

ABSTRACT

This monograph analyzes the civil liability of the State in relation to security incidents involving personal data managed by the National Council of Justice (CNJ). It begins by examining the historical development of State liability, from the theory of State irresponsibility to the consolidation of objective liability based on the administrative risk doctrine, as provided for in Article 37, paragraph 6, of the 1988 Federal Constitution. The study then investigates the legal protection of privacy and personal data within the Brazilian legal system, considering its connection with human dignity, personality rights, informational self-determination, and the regulatory framework established by the General Personal Data Protection Law (LGPD). It demonstrates that the CNJ, by coordinating and managing national databases of the Judiciary, acts as a controller of personal data and is therefore subject to the duties of security, prevention, and governance established by the LGPD and by its own institutional regulations. The concentration of procedural, criminal, family-related, property-related, and sensitive information increases the risks associated with unauthorized access and data breaches, requiring a level of protection compatible with the nature and relevance of the data processed. The study concludes that State civil liability in such cases does not arise automatically from the mere occurrence of a security incident. Rather, it depends on the establishment of the legal requirements for the duty to compensate, especially the existence of damage, a causal link, and a failure to comply with the legal duties of protection.

Keywords: civil liability of the State; personal data protection; LGPD; National Council of Justice; databases.

LISTA DE SIGLAS

ADI – Ação Direta de Inconstitucionalidade

ANPD – Autoridade Nacional de Proteção de Dados

CNJ – Conselho Nacional de Justiça

DataJud – Base Nacional de Dados do Poder Judiciário

LGPD – Lei Geral de Proteção de Dados Pessoais

SUMÁRIO

1 INTRODUÇÃO

A intensificação do uso de tecnologias da informação pelo Poder Público alterou significativamente a forma de organização e execução das atividades administrativas, ampliando o tratamento de dados pessoais em diversos setores estatais. No âmbito do Poder Judiciário, a informatização dos processos, a integração de sistemas e a formação de bases nacionais de dados passaram a desempenhar papel relevante para a gestão da atividade jurisdicional e para o planejamento das políticas judiciárias. Esse movimento atribuiu especial importância à proteção das informações sob custódia estatal, sobretudo diante da concentração de dados pessoais cuja utilização deve observar os parâmetros estabelecidos pelo ordenamento jurídico.

A crescente utilização de dados pessoais pela Administração Pública tornou mais evidente a necessidade de proteção jurídica dessas informações, especialmente após o reconhecimento da proteção de dados como direito fundamental pela Emenda Constitucional nº 115/2022. Essa tutela deixou de se limitar à preservação da intimidade para abranger o controle sobre o fluxo informacional e a salvaguarda da autodeterminação informativa, em razão da estreita relação entre os dados pessoais e o livre desenvolvimento da personalidade. A formação de bases públicas de abrangência nacional, por sua vez, potencializa os riscos inerentes ao tratamento dessas informações, pois amplia os impactos decorrentes de acessos não autorizados, vazamentos e outras falhas de segurança, impondo aos agentes estatais a observância de padrões rigorosos de proteção.

A relevância do tema decorre da posição assumida pelo Poder Judiciário na sociedade da informação, diante da expansão dos processos eletrônicos, da integração de sistemas e da formação de bases nacionais voltadas à gestão da atividade jurisdicional. A questão ganha contornos específicos na atuação do Conselho Nacional de Justiça, órgão responsável pela coordenação de políticas judiciárias e pela administração de relevantes bases nacionais de dados do Poder Judiciário.

A reunião de informações processuais e pessoais em sistemas como o DataJud, o Banco Nacional de Medidas Penais e Prisões, o Sistema Nacional de Adoção e Acolhimento e a plataforma Codex atribui ao Conselho a condição de controlador de dados pessoais, submetendo sua atuação às disposições da Lei Geral

de Proteção de Dados Pessoais. Diante dessa configuração, em que medida o Estado pode ser civilmente responsabilizado por incidentes de segurança envolvendo dados pessoais administrados pelo Conselho Nacional de Justiça, especialmente à luz dos deveres de proteção impostos pela Constituição Federal, pela Lei Geral de Proteção de Dados Pessoais e pelas normas internas do próprio órgão?

A pesquisa justifica-se sob o aspecto científico e prático por articular temas cuja análise integrada apresenta relevantes desafios jurídicos, especialmente quanto à incidência do regime da responsabilidade civil do Estado nas hipóteses de incidentes de segurança envolvendo o tratamento de dados pessoais realizado pelo Poder Judiciário. A análise da posição jurídica do Conselho Nacional de Justiça como controlador de bases nacionais e dos deveres que lhe são impostos pela Constituição Federal, pela Lei Geral de Proteção de Dados Pessoais e por sua regulamentação interna contribui para a compreensão dos limites jurídicos da atuação estatal na gestão dessas informações e dos pressupostos aplicáveis à reparação de eventuais danos decorrentes do descumprimento dessas obrigações.

O presente trabalho tem por objetivo explorar o regime jurídico da responsabilidade civil do Estado aplicável aos incidentes de segurança envolvendo os bancos de dados administrados pelo Conselho Nacional de Justiça. Para esse fim, aborda os fundamentos da responsabilidade civil estatal e sua disciplina constitucional; apresenta a evolução da proteção jurídica dos dados pessoais e o sistema instituído pela Lei Geral de Proteção de Dados Pessoais; investiga a posição do Conselho Nacional de Justiça como controlador de dados, os deveres de proteção decorrentes dessa condição e, por fim, delimita os pressupostos da responsabilização civil nas hipóteses de violação das obrigações de segurança relacionadas ao tratamento de dados pessoais.

A pesquisa adota o método dedutivo, com abordagem qualitativa e natureza bibliográfica e documental. O estudo utiliza como fontes a Constituição Federal, a Lei Geral de Proteção de Dados Pessoais, o Código Civil, resoluções do Conselho Nacional de Justiça, julgados do Supremo Tribunal Federal e do Superior Tribunal de Justiça, além da doutrina pertinente à responsabilidade civil do Estado e à proteção de dados pessoais. A partir da integração dessas fontes, busca-se delimitar o regime jurídico aplicável aos incidentes de segurança envolvendo os bancos de dados administrados pelo Conselho Nacional de Justiça e examinar as consequências

jurídicas decorrentes de eventual violação dos deveres de proteção impostos ao órgão.

A primeira seção apresenta os fundamentos teóricos da responsabilidade civil do Estado, partindo das principais teorias contratualistas acerca da formação do Estado para demonstrar a evolução histórica da responsabilização estatal. Na sequência, apresenta as teorias da responsabilidade civil, com destaque para as concepções subjetiva e objetiva, abordando seus pressupostos, fundamentos e hipóteses de incidência. Por fim, examina as excludentes de responsabilidade e a distinção entre as teorias do risco administrativo e do risco integral, delimitando o regime jurídico adotado pelo ordenamento constitucional brasileiro.

A segunda seção dedica-se à evolução da proteção jurídica dos dados pessoais, demonstrando a transição da concepção tradicional de privacidade para um modelo orientado pela autodeterminação informativa. Em seguida, examina o sistema brasileiro de proteção de dados, a partir da Constituição Federal, do Código Civil e da Lei Geral de Proteção de Dados Pessoais, destacando seus fundamentos, princípios, conceitos, agentes de tratamento e direitos dos titulares. Ao final, analisa a disciplina específica aplicável ao tratamento de dados pela Administração Pública, evidenciando os deveres impostos aos entes estatais no exercício de suas competências legais.

A terceira seção volta-se à atuação do Conselho Nacional de Justiça como agente de tratamento de dados pessoais, com destaque para sua condição de controlador das bases nacionais administradas pelo Poder Judiciário e para os deveres decorrentes dessa posição jurídica. Em seguida, examina a natureza das informações concentradas nesses sistemas e as obrigações de segurança previstas na Lei Geral de Proteção de Dados Pessoais, na regulamentação interna do Conselho e na jurisprudência constitucional. Por fim, investiga o regime jurídico da responsabilidade civil aplicável aos incidentes de segurança envolvendo esses bancos de dados, a partir da articulação entre a Constituição Federal e a Lei Geral de Proteção de Dados Pessoais, delimitando os pressupostos necessários à responsabilização estatal.

Com essa delimitação, a pesquisa concentra-se na análise da responsabilidade civil do Estado diante de incidentes de segurança envolvendo dados pessoais administrados pelo Conselho Nacional de Justiça. A investigação busca demonstrar que a proteção dessas informações não constitui apenas exigência técnica ou administrativa, mas dever jurídico vinculado à tutela dos direitos

fundamentais dos titulares. Assim, o estudo procura delimitar os pressupostos necessários à responsabilização estatal, considerando a atuação do CNJ como controlador de dados pessoais e os deveres de segurança impostos pelo ordenamento jurídico.

2 ORIGEM DO ESTADO E AS TEORIAS QUE FUNDAMENTAM A SUA RESPONSABILIDADE

Antes de analisar a responsabilidade civil do Estado, faz-se necessário o exame dos fundamentos que legitimam sua própria existência e do processo histórico de construção do dever de reparar os danos decorrentes de sua atuação. Nesse sentido, ao longo da evolução do Estado moderno, diferentes correntes doutrinárias buscaram explicar a origem do poder estatal e estabelecer os limites de sua atuação perante os indivíduos, contribuindo para o desenvolvimento dos modelos de responsabilização atualmente adotados pelo ordenamento jurídico brasileiro.

Nesse contexto, esta seção abordará, inicialmente, as teorias contratualistas que explicam a formação do Estado, para, em seguida, examinar a evolução das teorias da responsabilidade civil estatal, com ênfase nas concepções subjetiva e objetiva, culminando na disciplina conferida pela Constituição Federal de 1988.

2.1 Surgimento do Estado a partir das teorias contratualistas

A compreensão acerca da formação do Estado constitui elemento essencial para o estudo da responsabilidade civil estatal, tendo em vista que a própria ideia de responsabilização do poder público decorre da evolução histórica da organização política da sociedade. Nesse contexto, as teorias contratualistas desenvolvidas por Thomas Hobbes, John Locke e Jean-Jacques Rousseau desempenham papel fundamental na explicação da origem do Estado moderno, especialmente no que diz respeito à necessidade de superação do estado de natureza e instituição de uma autoridade política capaz de assegurar a convivência social.

A igualdade natural entre os homens, contudo, não conduz à harmonia social. Para Hobbes (2003), essa condição favorece a competição, a desconfiança e a busca pela supremacia, dando origem ao estado de natureza, caracterizado pela ausência de uma autoridade comum capaz de impor limites às ações humanas. Diante desse cenário de instabilidade, tornou-se necessária a instituição de um poder soberano destinado a assegurar a paz, a ordem e a segurança da coletividade.

Em razão disso, para Hobbes (2003), o Estado possui como finalidade primordial garantir a segurança e impedir o retorno ao estado de guerra. O soberano

concentra amplos poderes justamente para assegurar a ordem e a estabilidade social, sendo a autoridade estatal indispensável à preservação da vida humana. Diferentemente de Hobbes, John Locke apresenta uma visão mais otimista acerca do estado de natureza. Para o autor, os homens nascem livres, iguais e dotados de direitos naturais, dentre os quais se destacam a vida, a liberdade e a propriedade (Locke, 2006).

Dessa forma, Locke estabelece fundamentos importantes para o constitucionalismo moderno, especialmente no que diz respeito à limitação do poder político e à proteção das liberdades individuais (Locke, 2006). O Estado deixou de ser visto como autoridade absoluta e passa a ser compreendido como instrumento voltado à garantia dos direitos fundamentais. Jean-Jacques Rousseau, por sua vez, desenvolve a teoria contratualista a partir da ideia de soberania popular. O contrato social proposto por Rousseau (2006) não implica submissão irrestrita a um soberano absoluto, mas sim a constituição de uma vontade geral voltada ao interesse comum. Assim, a soberania pertence ao povo, sendo a coletividade responsável pela formação das leis e pela legitimação do poder político.

A teoria de Rousseau contribuiu significativamente para o desenvolvimento das ideias democráticas modernas, especialmente no que concerne à soberania popular e à participação coletiva na formação do Estado. (Rousseau, 2006). Observa-se, portanto, que as teorias contratualistas apresentam diferentes perspectivas acerca da origem e da finalidade do Estado. Enquanto Hobbes defende um poder soberano forte para assegurar a paz, Locke sustenta a limitação do poder político e a proteção dos direitos naturais, e Rousseau fundamenta o Estado na vontade geral e na soberania popular.

Apesar dessas diferenças, todos reconhecem que o Estado surge da necessidade de organização da vida em sociedade e da preservação dos indivíduos, fornecendo as bases para a compreensão da legitimidade do poder estatal. As teorias contratualistas evidenciam que a legitimidade do Estado está diretamente relacionada à proteção dos direitos dos indivíduos e à promoção do interesse coletivo. Nesse contexto, à medida que o poder estatal deixa de ser compreendido como absoluto e passa a submeter-se ao ordenamento jurídico, surge também a necessidade de estabelecer mecanismos que assegurem a responsabilização do Estado pelos danos decorrentes de sua atuação.

2.2 O Estado enquanto ente que pode ser responsabilizado

A responsabilidade civil do Estado representa importante instrumento de proteção dos administrados diante dos danos ocasionados pela atuação estatal. Sua construção teórica decorre de um longo processo histórico, marcado pela evolução das funções do Estado e pela necessidade de compatibilizar o exercício do poder público com a garantia dos direitos individuais (Di Pietro, 2023). Nesse contexto, surgiram diversas teorias destinadas a fundamentar a obrigação estatal de reparar prejuízos causados a terceiros. Inicialmente, prevaleceu a teoria da irresponsabilidade do Estado, fundada na ideia de soberania absoluta. Segundo essa concepção, o Estado, por representar autoridade soberana, não poderia ser responsabilizado pelos atos praticados por seus agentes (Meirelles, 2016).

Conforme explica Meirelles (2016), tal doutrina foi progressivamente abandonada pelos ordenamentos jurídicos ocidentais, especialmente após a edição do Crown Proceeding Act, na Inglaterra, em 1947, e do Federal Tort Claims Act, nos Estados Unidos, em 1946. Ainda segundo Meirelles (2016), “caíram, assim, os últimos redutos da irresponsabilidade civil do Estado pelos atos de seus agentes”. Com a superação da irresponsabilidade estatal, passaram a desenvolver-se as teorias civilistas da responsabilidade. Nesse período, buscava-se equiparar a responsabilidade do Estado à responsabilidade civil do particular, exigindo-se a demonstração de culpa para a configuração do dever de indenizar.

Conforme leciona Di Pietro (2023), “a regra adotada, por muito tempo, foi a da irresponsabilidade; caminhou-se, depois, para a responsabilidade subjetiva, vinculada à culpa” (Di Pietro, 2023, p. 1759). No âmbito das teorias civilistas, ganhou destaque a distinção entre atos de império e atos de gestão. Os atos de império eram praticados com prerrogativas típicas de autoridade estatal, enquanto os atos de gestão aproximavam-se das atividades exercidas pelos particulares (Meirelles, 2016). A responsabilidade estatal, nessa fase, somente era admitida em relação aos atos de gestão. Entretanto, a crescente complexidade das funções administrativas demonstrou a insuficiência dessa distinção para solucionar os conflitos decorrentes da atuação estatal.

Posteriormente, desenvolveram-se as teorias publicistas da responsabilidade civil do Estado, afastando-se a aplicação estrita dos princípios privatistas. Nesse sentido, Meirelles (2016) afirma que “não se pode equiparar o

Estado, com seu poder e seus privilégios administrativos, ao particular, despido de autoridade e de prerrogativas públicas" (Meirelles, 2016, p. 780). Assim, consolidou-se o entendimento de que a responsabilidade estatal deveria ser regida por princípios próprios do Direito Público. Dentre as teorias publicistas, destaca-se inicialmente a teoria da culpa administrativa, também denominada culpa do serviço ou faute du service. Tal teoria representa importante transição entre a responsabilidade subjetiva clássica e a responsabilidade objetiva.

Segundo Meirelles (2016), "a teoria da culpa administrativa representa o primeiro estágio da transição entre a doutrina subjetiva da culpa civil e a tese objetiva do risco administrativo" (Meirelles, 2016, p. 781). A culpa do serviço público caracteriza-se quando o serviço não funciona, funciona mal ou funciona de forma tardia. Conforme esclarece Di Pietro (2023), "essa culpa do serviço público ocorre quando: o serviço público não funcionou (omissão), funcionou atrasado ou funcionou mal" (Di Pietro, 2023, p. 1763). Embora represente avanço em relação à responsabilidade subjetiva tradicional, essa teoria ainda exige a demonstração de falha estatal.

Nesse mesmo sentido, Bandeira de Mello (2015) sustenta que a faute du service não constitui hipótese de responsabilidade objetiva. Para o autor, "é responsabilidade subjetiva porque baseada na culpa (ou dolo)" (Mello, 2015, p. 1032). Assim, mesmo afastando-se da análise individual da culpa do agente público, a teoria da culpa administrativa permanece vinculada à ideia de falha do serviço estatal. Com a ampliação das atividades desempenhadas pelo Estado e o fortalecimento das garantias individuais, consolidou-se a teoria da responsabilidade objetiva. Nessa concepção, a obrigação de indenizar decorre da mera relação causal entre a atuação estatal e o dano sofrido pelo administrado, independentemente de comprovação de culpa (Mello, 2015).

Conforme ensina Bandeira de Mello (2015), "responsabilidade objetiva é a obrigação de indenizar que incumbe a alguém em razão de um procedimento lícito ou ilícito que produziu uma lesão na esfera juridicamente protegida de outrem" (Mello, 2015, p. 1034). De igual modo, Di Pietro (2023) afirma que, nessa teoria, "a ideia de culpa é substituída pela de nexo de causalidade entre o funcionamento do serviço público e o prejuízo sofrido pelo administrado" (Di Pietro, 2023, p. 1764). A teoria objetiva fundamenta-se especialmente na ideia de risco administrativo.

Segundo Meirelles (2016), “a teoria do risco administrativo faz surgir a obrigação de indenizar do só ato lesivo e injusto causado à vítima pela Administração” (Meirelles, 2016, p. 781). Nessa hipótese, basta a demonstração do dano e do nexo causal, dispensando-se a comprovação de culpa da Administração Pública. Além disso, a responsabilidade objetiva encontra fundamento na repartição equitativa dos encargos sociais.

Para Bandeira de Mello (2015), o fundamento da responsabilidade estatal decorre do princípio da igualdade, especialmente quando determinados indivíduos suportam ônus excessivos em razão da atuação estatal. Assim, busca-se evitar que prejuízos decorrentes da atividade administrativa recaiam exclusivamente sobre determinados administrados. No Brasil, a consolidação da responsabilidade objetiva ocorreu com a Constituição Federal de 1946. Segundo Bandeira de Mello (2015), o artigo 194 daquele diploma “introduziu normativamente, entre nós, a teoria da responsabilidade objetiva” (Mello, 2015, p. 1057).

Atualmente, a matéria encontra previsão no artigo 37, § 6º, da Constituição Federal de 1988, que estabelece a responsabilidade das pessoas jurídicas de direito público e das pessoas jurídicas de direito privado prestadoras de serviços públicos pelos danos causados por seus agentes a terceiros. Por fim, a doutrina reconhece ainda a teoria do risco integral, considerada modalidade extremada da responsabilidade objetiva. Conforme explica Meirelles (2016), essa teoria imporia ao Estado o dever de indenizar independentemente da existência de causas excludentes de responsabilidade, razão pela qual foi considerada excessiva pela doutrina tradicional.

Contudo, Di Pietro (2023) observa que o ordenamento jurídico brasileiro admite hipóteses excepcionais de aplicação do risco integral, como nos casos de danos nucleares e determinados atos terroristas. Dessa forma, percebe-se que as teorias da responsabilidade do Estado refletem a própria evolução do Direito Administrativo e do Estado de Direito. A passagem da irresponsabilidade estatal para a responsabilidade objetiva evidencia o fortalecimento da proteção dos administrados e a submissão da Administração Pública aos princípios constitucionais da legalidade, igualdade e reparação dos danos injustamente suportados pelos particulares.

A evolução das teorias da responsabilidade civil do Estado evidencia a progressiva ampliação da proteção conferida aos administrados, passando da completa ausência de responsabilização para modelos cada vez mais voltados à

reparação dos danos decorrentes da atuação estatal. Todavia, a compreensão desse processo histórico exige o exame individual das principais correntes doutrinárias que marcaram essa evolução. Nesse contexto, impõe-se iniciar pela teoria subjetiva, que representou o primeiro modelo efetivo de responsabilização do Estado após a superação da teoria da irresponsabilidade e estabeleceu importantes fundamentos para o desenvolvimento das concepções publicistas posteriormente consolidadas.

2.2.1 Teoria da Responsabilidade Subjetiva

A teoria subjetiva da responsabilidade civil do Estado fundamenta-se na necessidade de demonstração de culpa ou dolo para que surja o dever estatal de indenizar os danos causados aos particulares (Mello, 2015). Trata-se de concepção influenciada pelo Direito Civil clássico, na qual a responsabilização depende da comprovação de comportamento culposo imputável ao agente estatal ou à própria Administração Pública. Historicamente, a teoria subjetiva desenvolveu-se após o declínio da teoria da irresponsabilidade do Estado. Nesse período, buscou-se aproximar a responsabilidade estatal da responsabilidade aplicável aos particulares, submetendo o Poder Público às mesmas exigências de demonstração de culpa existentes nas relações privadas (Meirelles, 2016).

Conforme explica Di Pietro (2023), “a regra adotada, por muito tempo, foi a da irresponsabilidade; caminhou-se, depois, para a responsabilidade subjetiva, vinculada à culpa” (Di Pietro, 2023, p. 1759). No ordenamento jurídico brasileiro, a teoria subjetiva recebeu forte influência do artigo 15 do Código Civil de 1916. Segundo Meirelles (2016), referido dispositivo “acolhendo a doutrina subjetivista dominante em sua época, estabeleceu [...] que as pessoas jurídicas de Direito Público são civilmente responsáveis por atos de seus representantes” quando agissem de forma contrária ao direito ou faltando a dever legal (Meirelles, 2016, p. 783). Nesse modelo, exigia-se a comprovação da culpa da Administração para a configuração da responsabilidade civil estatal.

A responsabilidade subjetiva pressupõe, portanto, a existência de conduta culposa ou dolosa capaz de ocasionar dano ao administrado. Nesse sentido, Bandeira de Mello (2015) define a responsabilidade subjetiva como “a obrigação de indenizar que incumbe a alguém em razão de um procedimento contrário ao Direito – culposo

ou doloso – consistente em causar um dano a outrem ou em deixar de impedi-lo quando obrigado a isto” (Mello, 2015, p. 1031).

Embora inicialmente vinculada à culpa individual do agente público, a evolução doutrinária conduziu ao desenvolvimento da chamada teoria da culpa administrativa, também denominada culpa do serviço ou faute du service. Tal teoria representou importante avanço na responsabilização estatal, pois deslocou o foco da análise da culpa pessoal do agente para a verificação do funcionamento inadequado do serviço público. Conforme ensina Meirelles (2016), “a teoria da culpa administrativa representa o primeiro estágio da transição entre a doutrina subjetiva da culpa civil e a tese objetiva do risco administrativo” (Meirelles, 2016, p. 781). Nessa concepção, a responsabilidade decorre da falha estatal na prestação do serviço público, independentemente da identificação do agente responsável pelo dano.

A culpa do serviço público caracteriza-se quando o serviço não funciona, funciona mal ou funciona de maneira tardia. Segundo Di Pietro (2023), “essa culpa do serviço público ocorre quando: o serviço público não funcionou (omissão), funcionou atrasado ou funcionou mal” (Di Pietro, 2023, p. 1763). Assim, a responsabilidade estatal decorre da deficiência na atuação administrativa, configurando-se verdadeira culpa anônima da Administração Pública. Da mesma forma, Bandeira de Mello (2015) afirma que a faute du service “ocorre quando este não funciona, devendo funcionar, funciona mal ou funciona atrasado” (Mello, 2015, p. 1031). O autor ressalta, entretanto, que essa modalidade não constitui hipótese de responsabilidade objetiva, pois permanece fundamentada na ideia de culpa estatal. Nesse sentido, sustenta expressamente que “é responsabilidade subjetiva porque baseada na culpa (ou dolo) ” (Mello, 2015, p. 1032).

A teoria subjetiva apresenta especial relevância nos casos de omissão estatal. Parte significativa da doutrina entende que, nas hipóteses omissivas, não basta a simples ocorrência do dano para caracterizar a responsabilidade do Estado, sendo necessária a comprovação de falha do serviço público. Isso ocorre porque a omissão estatal exige a demonstração de que o Poder Público possuía dever jurídico de agir para evitar o resultado lesivo. Nesse sentido, Bandeira de Mello (2015) sustenta que “a responsabilidade do Estado é objetiva no caso de comportamento danoso comissivo e subjetiva no caso de comportamento omissivo” (Mello, 2015, p. 1045). Para o autor, a omissão estatal somente gera responsabilidade quando

caracterizada a culpa administrativa decorrente do não funcionamento, funcionamento defeituoso ou retardado do serviço público.

Di Pietro (2023) compartilha entendimento semelhante ao afirmar que, nos casos de omissão, “a responsabilidade é subjetiva, aplicando-se a teoria da culpa do serviço público ou da culpa anônima do serviço público” (Di Pietro, 2023, p. 1777). A autora destaca ainda que a omissão deve ser ilícita para gerar o dever de indenizar, exigindo-se a demonstração de que o Estado deixou de cumprir obrigação legal de agir. Além disso, Meirelles (2016) observa que a teoria da culpa administrativa ainda impõe relevante ônus probatório à vítima, uma vez que o particular deve demonstrar a falha do serviço público para obter a reparação do dano. Segundo o autor, “esta teoria ainda pede muito da vítima, que, além da lesão sofrida injustamente, fica no dever de comprovar a falta do serviço para obter a indenização” (Meirelles, 2016, p. 781).

Apesar das limitações da teoria subjetiva, sua importância permanece significativa no Direito Administrativo contemporâneo, especialmente nas hipóteses de responsabilidade decorrente de omissão estatal. A necessidade de demonstração da culpa administrativa busca impedir a responsabilização indiscriminada do Estado por todo e qualquer dano sofrido pelos administrados, preservando o equilíbrio entre o dever de reparação e os limites da atuação estatal. Dessa forma, a teoria subjetiva representa etapa fundamental na evolução da responsabilidade civil do Estado, contribuindo para a superação da irresponsabilidade estatal e para o desenvolvimento das modernas teorias publicistas da responsabilidade administrativa.

Contudo, embora a teoria subjetiva tenha representado um avanço crucial na superação da irresponsabilidade estatal, a imposição de um severo ônus probatório ao particular e a crescente complexidade das funções públicas demonstraram as limitações desse modelo para garantir uma proteção integral ao administrado. Diante da dificuldade prática enfrentada pelas vítimas para comprovar a falha ou a culpa anônima do serviço em um Estado em constante expansão de suas atividades, a doutrina publicista viu-se diante da necessidade de conceber critérios de responsabilização mais amplos e eficazes. É nesse contexto de evolução jurídica e de busca por maior equidade que emerge a teoria objetiva, inaugurando uma sistemática que dispensa a verificação de culpa e se fundamenta diretamente no risco e no nexo causal.

2.2.2 Teoria da Responsabilidade Objetiva

A teoria objetiva da responsabilidade civil do Estado fundamenta-se na ideia de que o dever de indenizar surge independentemente da comprovação de culpa da Administração Pública ou de seus agentes. Nessa concepção, basta a demonstração da ocorrência do dano e da existência de nexo causal entre a atuação estatal e o prejuízo suportado pelo particular para que se configure a obrigação de reparação. O desenvolvimento da responsabilidade objetiva decorreu da insuficiência da teoria subjetiva para assegurar proteção adequada aos administrados diante da crescente ampliação das atividades desempenhadas pelo Estado. A complexidade das funções administrativas e a dificuldade enfrentada pelas vítimas para comprovar a culpa estatal impulsionaram a construção de teorias fundadas em critérios objetivos de responsabilização (Meirelles, 2016).

Segundo Bandeira de Mello (2015), “responsabilidade objetiva é a obrigação de indenizar que incumbe a alguém em razão de um procedimento lícito ou ilícito que produziu uma lesão na esfera juridicamente protegida de outrem” (Mello, 2015, p. 1034). Nessa perspectiva, a responsabilidade estatal decorre da simples relação causal entre a atividade administrativa e o dano causado ao administrado. De igual modo, Di Pietro (2023) afirma que, na teoria objetiva, “a ideia de culpa é substituída pela de nexo de causalidade entre o funcionamento do serviço público e o prejuízo sofrido pelo administrado” (Di Pietro, 2023, p. 1764). Assim, a responsabilidade civil do Estado passa a fundamentar-se no risco inerente à atuação administrativa, dispensando-se a demonstração de dolo ou culpa do agente público.

No ordenamento jurídico brasileiro, a teoria objetiva encontra fundamento principalmente na teoria do risco administrativo. Conforme explica Meirelles (2016), “a teoria do risco administrativo faz surgir a obrigação de indenizar do só ato lesivo e injusto causado à vítima pela Administração” (Meirelles, 2016, p. 781). Nesse modelo, exige-se apenas a comprovação do dano e do nexo causal entre a atuação estatal e a lesão sofrida pelo particular. A teoria do risco administrativo baseia-se na ideia de que a atuação estatal gera riscos para os administrados, razão pela qual o Estado deve suportar os ônus decorrentes de sua própria atividade.

Nesse sentido, Meirelles (2016) afirma que tal teoria “baseia-se no risco que a atividade pública gera para os administrados e na possibilidade de acarretar dano a certos membros da comunidade” (meirelles, 2016, p. 781). Além disso, a

responsabilidade objetiva encontra fundamento no princípio da igualdade, especialmente na repartição equitativa dos encargos sociais. Segundo Bandeira de Mello (2015), quando a atuação estatal impõe prejuízo anormal a determinado indivíduo em benefício da coletividade, surge para o Estado o dever de reparar o dano, evitando que um único administrado suporte ônus excessivo decorrente da atividade pública.

A configuração da responsabilidade objetiva do Estado depende da presença de determinados requisitos. Conforme leciona Meirelles (2016), essa modalidade de responsabilidade é composta pelos seguintes elementos: “(a) a alteridade do dano, (b) a causalidade material entre o *eventus damni* e o comportamento positivo ou negativo do agente público, (c) a oficialidade da atividade causal e lesiva imputável a agente do Poder Público [...], e (d) a ausência de causa excludente da responsabilidade estatal” (Meirelles, 2016, p. 789).

Dessa forma, cabe ao prejudicado, demonstrar a ocorrência do dano e o nexo causal entre a atuação administrativa e o prejuízo sofrido. Conforme destaca Meirelles (2016), “para obter a indenização basta que o lesado acione a Fazenda Pública e demonstre o nexo causal entre o fato lesivo [...] e o dano” (Meirelles, 2016, p. 790). Entretanto, a teoria do risco administrativo não implica responsabilização absoluta do Estado. Diferentemente do risco integral, admite-se a existência de causas excludentes ou atenuantes da responsabilidade civil estatal. Nesse sentido, Meirelles (2016) esclarece que “o risco administrativo não significa que a Administração deva indenizar sempre e em qualquer caso o dano suportado pelo particular” (Meirelles, 2016, p. 782).

Assim, a culpa exclusiva da vítima, a culpa de terceiros, a força maior e a ausência de nexo causal podem excluir ou reduzir a responsabilidade estatal. Segundo Di Pietro (2023), a principal diferença entre o risco administrativo e o risco integral reside justamente na admissibilidade das causas excludentes de responsabilidade (Di Pietro, 2023). Por outro lado, a teoria do risco integral representa modalidade extremada da responsabilidade objetiva. Nessa hipótese, o Estado responde independentemente da existência de causas excludentes, assumindo integralmente os riscos da atividade desenvolvida.

Conforme explica Meirelles (2016), essa teoria “ficaria obrigada a indenizar todo e qualquer dano suportado por terceiros, ainda que resultante de culpa ou dolo da vítima” (Meirelles, 2016, p. 782). Embora tradicionalmente rejeitada pela doutrina

majoritária, o ordenamento jurídico brasileiro admite hipóteses excepcionais de aplicação do risco integral. Di Pietro (2023) menciona os casos de danos decorrentes de acidentes nucleares e determinados atos terroristas contra aeronaves brasileiras como situações em que o sistema jurídico admite responsabilização integral do Estado.

Nesse sentido, Meirelles (2016) esclarece que, “enquanto para a Administração a responsabilidade independe da culpa, para o servidor a responsabilidade depende da culpa” (Meirelles, 2016, p. 792). Assim, o Estado indeniza o particular prejudicado e, posteriormente, pode buscar o ressarcimento perante o agente público responsável pelo dano. Portanto, a teoria objetiva representa importante avanço na proteção dos administrados frente à atuação estatal, facilitando a reparação dos danos decorrentes da atividade administrativa. Sua consolidação evidencia o fortalecimento do Estado de Direito e a submissão da Administração Pública aos princípios constitucionais da legalidade, igualdade e responsabilidade estatal.

2.3 Responsabilidade Civil do Estado na Constituição Federal de 1988

A sistemática da responsabilidade civil do Estado no ordenamento jurídico brasileiro encontra seu alicerce fundamental no artigo 37, § 6º, da Constituição Federal de 1988. Referido dispositivo consagrou a responsabilidade objetiva da Administração Pública pelos danos que seus agentes, nessa qualidade, causarem a terceiros, assegurando o posterior direito de regresso contra o responsável nos casos de dolo ou culpa (BRASIL, 1988). Tal previsão constitui essencial mecanismo de proteção dos administrados, consolidando a evolução histórica que, conforme leciona Di Pietro (2023), superou as teorias de irresponsabilidade para adotar o modelo pautado no risco administrativo.

Para Bandeira de Mello (2015), a responsabilidade civil estatal deriva diretamente dos princípios da legalidade, da igualdade e da indisponibilidade do interesse público, visto que não seria juridicamente admissível transferir ao indivíduo prejuízos oriundos de atividades desenvolvidas em benefício da coletividade. Dessa forma, a responsabilidade objetiva do Estado atua como instrumento de preservação do equilíbrio nas relações entre o Poder Público e os administrados. A responsabilidade objetiva de matriz constitucional aplica-se tanto às pessoas jurídicas

de direito público quanto às de direito privado prestadoras de serviços públicos, abrangendo atos comissivos praticados por agentes no exercício de suas funções (Meirelles, 2016).

Contudo, a doutrina reconhece hipóteses excludentes ou atenuantes que rompem ou mitigam o nexo causal necessário à configuração do dever de indenizar. Referida responsabilidade abrange atos administrativos, legislativos e, em situações excepcionais, jurisdicionais, desde que presentes os requisitos para a configuração do dever de indenizar. A jurisprudência consolidou o entendimento de que tal responsabilidade alcança usuários e terceiros não usuários afetados pela atividade, ampliando a proteção jurídica conferida aos cidadãos (Meirelles, 2016). O direito de regresso contra o agente público constitui relevante mecanismo previsto na Constituição, permitindo que a Administração busque o ressarcimento de indenizações pagas a terceiros, desde que provado o dolo ou a culpa funcional (Brasil, 1988).

Conforme ensina Di Pietro (2023), o regresso possui dupla finalidade: proteger o administrado, facilitando a reparação direta pelo Estado, e impedir a irresponsabilidade do agente público, que sabe do dever de ressarcir prejuízos causados por sua conduta culposa. Sob essa perspectiva, a ação regressiva depende da demonstração do pagamento da indenização, da existência do dano e da conduta dolosa ou culposa do agente. Não basta a mera ocorrência do prejuízo para que o servidor seja compelido ao ressarcimento, sendo indispensável a prova do elemento subjetivo em sua atuação funcional.

Segundo Meirelles (2016), o direito de regresso constitui garantia de proteção ao patrimônio público e de responsabilização ética do agente estatal. Funciona como instrumento indispensável de controle interno e de preservação da probidade administrativa, assegurando que a eficiência e a justiça orientem a atuação no âmbito do Estado Democrático de Direito. Já em relação à omissão, a matéria apresenta maior complexidade, pois o texto constitucional não distinguiu expressamente atos comissivos e omissivos. Consolidou-se o entendimento de que a omissão estatal enseja responsabilidade subjetiva, exigindo a prova da culpa administrativa ou falha do serviço, caracterizada pela negligência ou imperícia da Administração (Mello, 2015).

Para Bandeira de Mello (2015), a omissão gera dever de indenizar quando o Estado deixa de atuar eficientemente em face de uma obrigação específica de

impedir o dano, configurando a faute du service. Situações de falha na segurança ou na custódia de pessoas podem ensejar tal responsabilização, desde que demonstrada a omissão culposa e o nexo causal com o prejuízo sofrido. Diferencia-se a omissão genérica da omissão específica, sendo esta última mais apta a configurar o dever de indenizar (Di Pietro, 2023). Em ambos os casos, admitem-se as excludentes como a força maior ou a culpa da vítima para romper o liame causal e afastar a obrigação estatal de reparação.

Desta feita, as excludentes da responsabilidade civil representam mecanismos destinados a limitar o dever de indenizar quando rompido o nexo causal, sendo fundamentais para a correta aplicação da teoria do risco administrativo (Brasil, 1988). Embora a regra seja a objetividade, o Estado não responde de forma absoluta por todos os danos sociais ocorridos sem sua intervenção direta. Conforme ensina Di Pietro (2023), as principais causas excludentes são a culpa exclusiva da vítima, o caso fortuito, a força maior e o fato de terceiro. Tais situações impedem a configuração do nexo de causalidade necessário à responsabilização. A culpa exclusiva da vítima afasta integralmente a responsabilidade, enquanto a culpa concorrente permite a redução proporcional da indenização.

O caso fortuito e a força maior referem-se a eventos inevitáveis e alheios à vontade estatal. A doutrina distingue o fortuito interno, ligado ao risco da atividade, do fortuito externo, estranho à atuação administrativa e mais apto a excluir o dever de indenizar (Di Pietro, 2023). Já o fato de terceiro rompe o vínculo causal quando a conduta de outrem é a causa única do prejuízo (Meirelles, 2016). A disciplina constitucional da responsabilidade civil do Estado evidencia que o dever de indenizar decorre da violação de direitos juridicamente tutelados, desde que presentes os pressupostos estabelecidos pelo ordenamento.

Contudo, para a adequada compreensão da responsabilidade estatal no contexto da Lei Geral de Proteção de Dados Pessoais, mostra-se necessário identificar, previamente, quais direitos são objeto de proteção quando a Administração Pública realiza o tratamento de dados pessoais. Nesse cenário, destaca-se a privacidade como um dos principais bens jurídicos tutelados pela LGPD, cuja evolução conceitual e fundamento constitucional revelam a estreita relação entre a proteção dos dados pessoais, a dignidade da pessoa humana e o livre desenvolvimento da personalidade.

3 A PRIVACIDADE COMO COROLÁRIO DE PROTEÇÃO DA LGPD

As profundas transformações provocadas pelo avanço das tecnologias da informação modificaram significativamente a forma como a privacidade é compreendida e protegida pelo Direito. A concepção tradicional, que associava a privacidade ao direito de ser deixado só e à possibilidade de manter determinados aspectos da vida afastados do conhecimento de terceiros, mostrou-se insuficiente diante de uma realidade marcada pela intensa coleta, processamento e circulação de informações pessoais. Segundo Doneda (2020, p. 25), a tutela da privacidade baseada no isolamento e na reclusão já não oferece parâmetros adequados para um contexto em que o fluxo de informações cresce continuamente e as tecnologias ampliam as possibilidades de interferência na esfera privada dos indivíduos.

Nesse cenário, a proteção jurídica da pessoa passou a exigir uma abordagem mais ampla, capaz de enfrentar os desafios decorrentes da sociedade da informação. A preocupação deixou de se concentrar exclusivamente na preservação do segredo ou da intimidade para incorporar questões relacionadas ao controle sobre os dados pessoais e à forma como eles circulam entre instituições públicas e privadas. Segundo Doneda (2020, p. 39), a privacidade passou a se estruturar em torno do eixo “pessoa-informação-circulação-controle”, substituindo gradativamente o paradigma anteriormente centrado na relação entre pessoa, informação e sigilo.

Em sentido semelhante, Bioni (2021, p. 126) sustenta que a evolução do direito à privacidade representa a passagem de uma liberdade meramente negativa para uma liberdade positiva, fundada na possibilidade de o indivíduo participar das decisões relacionadas às suas informações pessoais.Essa mudança encontra fundamento na ideia de autodeterminação informativa, concebida como o direito de o indivíduo decidir quando e em que medida seus dados pessoais podem ser utilizados (Doneda, 2020, p. 160).

Historicamente, a proteção de dados pessoais foi construída a partir da compreensão de que o titular deve possuir algum grau de controle sobre o fluxo de suas informações, razão pela qual o consentimento assumiu posição de destaque nos modelos regulatórios contemporâneos (Bioni, 2021, p. 29). Mais do que um instrumento de proteção da privacidade, a autodeterminação informativa passou a ser reconhecida como expressão da liberdade individual e da própria personalidade humana (Doneda, 2020).

A relevância dessa proteção torna-se ainda mais evidente quando se observa que os dados pessoais passaram a representar verdadeiras projeções digitais dos indivíduos. Doneda (2020, p. 25) destaca que, em diversos contextos, as pessoas são avaliadas a partir de informações armazenadas em bancos de dados, que funcionam como uma espécie de “avatar” digital. Da mesma forma, Bioni (2021, p. 121) afirma que a crescente datificação das relações sociais produz uma verdadeira “biografia digital”, composta pelo conjunto de informações que identificam e descrevem cada pessoa. Em consequência, a utilização inadequada desses dados pode comprometer não apenas a privacidade, mas também a autonomia, a liberdade e o livre desenvolvimento da personalidade.

Diante dessa realidade, a tutela informacional passou a ser compreendida como um direito fundamental autônomo, destinado a assegurar que o fluxo informacional não se torne um fator de restrição da liberdade humana (Bioni, 2021). Como observa Bioni (2021, p. 123), a tutela dos dados pessoais constitui uma nova fronteira dos direitos da personalidade, voltada à preservação da autodeterminação do indivíduo em uma sociedade cada vez mais orientada pelo tratamento de informações. Essa evolução doutrinária foi gradualmente incorporada ao ordenamento jurídico brasileiro, acompanhando as transformações tecnológicas e a intensificação do tratamento de dados pessoais por agentes públicos e privados. À medida em que os riscos decorrentes da circulação de informações se tornaram mais evidentes, consolidou-se a necessidade de um regime jurídico específico voltado à proteção dos titulares de dados (Doneda, 2020).

Esse processo culminou na promulgação da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais), que estabeleceu como fundamentos da disciplina a tutela da liberdade, da privacidade e do livre desenvolvimento da personalidade (Bioni, 2021). Posteriormente, a Emenda Constitucional nº 115/2022 reforçou essa proteção ao reconhecer expressamente o direito à proteção informacional como direito fundamental, mediante sua inclusão no artigo 5º da Constituição Federal. A consolidação desse regime jurídico representa importante marco na proteção dos direitos da personalidade, ao estabelecer princípios, direitos e deveres aplicáveis ao tratamento de dados pessoais.

Além de disciplinar a atuação dos agentes de tratamento, esse conjunto normativo fornece os parâmetros que orientam a tutela jurídica dos dados pessoais e servem de fundamento para a responsabilização decorrente de seu tratamento ilícito,

inclusive quando praticado pela Administração Pública, tema que será desenvolvido nos capítulos seguintes. A incorporação desse modelo ao ordenamento jurídico brasileiro ocorreu de forma gradual, por meio da interação entre normas constitucionais, civis e infraconstitucionais que passaram a conferir proteção específica aos dados pessoais. Assim, para compreender os fundamentos jurídicos dessa tutela, torna-se necessário examinar os principais diplomas que compõem o sistema brasileiro de proteção de dados pessoais.

3.1 A Proteção de Dados Pessoais no Sistema Jurídico Brasileiro

A proteção de dados pessoais no ordenamento jurídico brasileiro não decorre de um único diploma normativo, mas de um conjunto de normas e princípios que, de forma integrada, asseguram a tutela das informações pessoais. Esse sistema é estruturado a partir da Constituição Federal, que estabelece os direitos fundamentais relacionados à privacidade e à proteção de dados, do Código Civil, que disciplina os direitos da personalidade, e da Lei Geral de Proteção de Dados Pessoais (LGPD), responsável por instituir um regime jurídico específico para o tratamento de dados pessoais.

A análise desses instrumentos revela a evolução da proteção jurídica conferida às informações pessoais e fornece a base normativa necessária para a compreensão dos mecanismos institucionais e da responsabilidade decorrente de sua violação.

3.1.1 Fundamentos da privacidade na Constituição Federal de 1988

A salvaguarda de dados pessoais no ordenamento jurídico brasileiro possui fundamento constitucional e encontra respaldo em diversos dispositivos da Constituição Federal de 1988. Embora o texto constitucional originário não previsse expressamente a proteção de dados como direito fundamental autônomo, a tutela das informações pessoais sempre esteve associada à dignidade da pessoa humana, à intimidade, à vida privada e às liberdades individuais, valores estruturantes do Estado Democrático de Direito (Brasil, 1988).

O fundamento constitucional mais amplo da tutela de dados pessoais encontra-se no princípio da dignidade da pessoa humana, previsto no artigo 1º, inciso

III, da Constituição Federal de 1988. Como ensina Sarlet (2021), a dignidade constitui valor-fonte do sistema constitucional brasileiro e parâmetro interpretativo para a proteção dos direitos fundamentais e para a limitação da atuação estatal. Nesse contexto, a proteção das informações pessoais visa impedir que o indivíduo seja reduzido a mero objeto de tratamento informacional, preservando sua autonomia e seu livre desenvolvimento da personalidade (Bioni, 2021).

Além desse fundamento geral, a Constituição assegura proteção específica à esfera privada. O artigo 5º, inciso X, consagra a inviolabilidade da intimidade, da vida privada, da honra e da imagem, com direito à indenização por dano material ou moral decorrente de sua violação (Brasil, 1988). Embora formulado em contexto anterior à sociedade digital, o dispositivo passou a servir de base para a tutela contra interferências indevidas na esfera informacional dos indivíduos. A Constituição de 1988 também protege o sigilo das comunicações, ao estabelecer, no artigo 5º, inciso XII, a inviolabilidade da correspondência, das comunicações telegráficas, de dados e das comunicações telefônicas, ressalvadas as hipóteses legais (Brasil, 1988).

O dispositivo reforça a preocupação constitucional com a confidencialidade das informações pessoais e com a limitação de acessos indevidos, inclusive em ambientes digitais. Outro instrumento constitucional relevante é o habeas data, previsto no artigo 5º, inciso LXXII, da Constituição Federal. Tal garantia permite ao indivíduo obter informações relativas à sua pessoa constantes de registros ou bancos de dados de entidades governamentais ou de caráter público, bem como promover sua retificação quando necessário (Brasil, 1988).

De acordo com Doneda (2020, p. 285), o habeas data representou uma das primeiras manifestações normativas brasileiras voltadas especificamente à proteção das informações pessoais, demonstrando a preocupação constitucional com o controle dos dados pelos próprios titulares. A proteção constitucional dos dados pessoais foi significativamente fortalecida com a promulgação da Emenda Constitucional nº 115, de 2022, que introduziu o inciso LXXIX ao artigo 5º da Constituição Federal, estabelecendo expressamente que "é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais" (Brasil, 2022). A partir dessa alteração, esse resguardo passou a integrar formalmente o catálogo dos direitos fundamentais, consolidando entendimento já reconhecido pela doutrina e pela jurisprudência constitucional.

O reconhecimento expresso da proteção de dados como direito fundamental possui especial relevância para a atuação estatal. Como destaca Sarlet (2021), os direitos fundamentais têm não apenas dimensão subjetiva, ligada às pretensões individuais dos titulares, mas também dimensão objetiva, que irradia efeitos sobre toda a atuação dos poderes públicos. Dessa dimensão decorrem deveres de proteção do Estado, que impõem a adoção de medidas destinadas a prevenir violações e assegurar a efetividade desses direitos (Sarlet, 2021, p. 128).

Sob essa perspectiva, tais deveres ganham relevo com a digitalização da Administração Pública e o uso de extensas bases governamentais. Deste modo, como os órgãos estatais tratam informações relativas à saúde, previdência, segurança pública, tributação e atividade jurisdicional, a proteção desses dados não constitui mera faculdade administrativa, mas dever constitucional voltado à salvaguarda dos direitos fundamentais dos titulares (Sarlet, 2021).

À luz dessas considerações, a Constituição Federal de 1988 fornece as bases normativas essenciais da proteção de dados no Brasil, e confere densidade jurídica ao dever estatal de resguardar informações sob sua custódia. Como se verá adiante, também está presente na legislação infraconstitucional o dever de salvaguarda dos dados pessoais dos cidadãos. A partir dessas premissas, o Código Civil de 2002 ocupa posição de destaque ao disciplinar os direitos da personalidade e prever instrumentos destinados à prevenção e à reparação de lesões decorrentes da violação da esfera privada, complementando a proteção assegurada pela Constituição Federal.

3.1.2 A proteção de dados pessoais no Código Civil Brasileiro

A tutela de dados pessoais no ordenamento jurídico brasileiro não se restringe à Constituição e à LGPD, encontrando também fundamento relevante no Código Civil. Embora elaborado antes da consolidação da sociedade da informação, o Código Civil de 2002 incorporou mecanismos de tutela da personalidade humana que oferecem base normativa para a proteção da privacidade, da intimidade e das informações pessoais. A disciplina dos direitos da personalidade ocupa posição central nesse contexto. Os artigos 11 a 21 do Código Civil estabelecem um conjunto de garantias voltadas à proteção dos atributos essenciais da pessoa humana,

reconhecendo que determinados direitos possuem natureza extrapatrimonial e são indispensáveis à preservação da dignidade do indivíduo (Brasil, 2002).

Tais direitos caracterizam-se pela intransmissibilidade, irrenunciabilidade e indisponibilidade relativa, refletindo a compreensão de que a pessoa humana constitui valor central do ordenamento jurídico. Entre os dispositivos mais relevantes para a tutela de dados pessoais destaca-se o artigo 21 do Código Civil, segundo o qual "a vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma" (Brasil, 2002). Embora concebido em momento anterior à expansão dos ambientes digitais, o dispositivo abrange, em interpretação contemporânea, a coleta, o armazenamento, o compartilhamento e a divulgação indevida de informações pessoais.

A evolução tecnológica ampliou os desafios ligados à preservação da esfera privada. Como observa Doneda, o desenvolvimento das tecnologias de informação transformou os dados pessoais em importante instrumento de poder, capaz de influenciar decisões e afetar diretamente a autonomia dos indivíduos (Doneda, 2020). Nesse cenário, a tutela dos direitos da personalidade impede que as informações pessoais sejam utilizadas de modo incompatível com a dignidade da pessoa humana e com o livre desenvolvimento da personalidade.

A tutela civil da privacidade também se relaciona diretamente com a responsabilidade civil decorrente da violação dos direitos da personalidade. O Código Civil estabelece, em seus artigos 186 e 927, que aquele que causar dano a outrem por ação ou omissão ilícita fica obrigado a repará-lo (Brasil, 2002). Assim, a utilização indevida de dados pessoais, a divulgação não autorizada de informações privadas ou a ocorrência de vazamentos capazes de comprometer a esfera jurídica do titular podem ensejar o dever de indenizar, especialmente quando configurados danos materiais ou morais decorrentes da violação da privacidade (DONEDA, 2020).

A proteção conferida pelo Código Civil complementa o sistema de tutela de dados ao assegurar mecanismos de tutela e reparação aplicáveis às hipóteses de lesão aos direitos da personalidade. Como destaca Sarlet, a dignidade da pessoa humana fundamenta esses direitos e orienta a interpretação das normas voltadas à proteção da esfera existencial do indivíduo (Sarlet, 2021). O resguardo dos dados pessoais, portanto, não se limita à dimensão patrimonial das informações, alcançando valores ligados à liberdade, à autonomia e à própria identidade da pessoa.

Nessa linha, a entrada em vigor da Lei Geral de Proteção de Dados (LGPD) não afastou a incidência das normas civis relativas à proteção da personalidade. Ao contrário, a lei passou a atuar de forma complementar ao Código Civil enquanto fornece disciplina específica para o tratamento de dados pessoais, os direitos da personalidade seguem oferecendo fundamento para a tutela da privacidade e para a reparação dos danos decorrentes de sua violação. No âmbito da Administração Pública, a relevância dessas disposições é ainda mais evidente diante do tratamento massivo de informações pelos órgãos estatais.

A exposição indevida de dados sob custódia do Poder Público pode representar não apenas descumprimento de deveres previstos na LGPD, mas, também, violação aos direitos da personalidade protegidos pelo Código Civil, hipótese em que a tutela civil da privacidade e o regime da responsabilidade civil assumem papel central (Doneda, 2020). Em consequência, o Código Civil integra o sistema brasileiro de proteção de dados ao assegurar tutela à vida privada, aos direitos da personalidade e à dignidade da pessoa humana. Suas disposições oferecem fundamento para a proteção das informações pessoais e para a responsabilização decorrente de sua utilização indevida, abrindo caminho para o exame dos órgãos estatais incumbidos de fiscalizar, regulamentar e tutelar esse direito.

Embora o Código Civil tenha desempenhado papel relevante ao fortalecer a tutela dos direitos da personalidade, sua disciplina não foi concebida para enfrentar as complexidades inerentes ao tratamento de dados pessoais na sociedade da informação. A crescente circulação de informações em ambiente digital, aliada à intensificação da coleta, do armazenamento e do compartilhamento de dados por agentes públicos e privados, evidenciou a necessidade de um regime jurídico específico capaz de disciplinar essas atividades de forma sistemática. Diante desse panorama, foi promulgada a Lei nº 13.709/2018, denominada Lei Geral de Proteção de Dados Pessoais (LGPD), responsável por consolidar um marco normativo voltado à proteção dos dados pessoais no ordenamento jurídico brasileiro.

3.1.3 Da Lei Geral de Proteção de Dados (Lei n° 13.709/2018)

É sabido que a tutela jurídica clássica mostrava-se insuficiente para enfrentar os desafios decorrentes da sociedade da informação. Embora a Constituição Federal e o Código Civil assegurassem a proteção da privacidade e dos direitos da

personalidade, essas normas não disciplinavam de forma específica o tratamento de dados pessoais. A intensificação da circulação de informações em ambiente digital evidenciou as limitações desse modelo de proteção. Na visão de Doneda (2020), esse novo contexto passou a exigir instrumentos jurídicos próprios, uma vez que a tutela baseada exclusivamente em mecanismos reparatórios já não se mostrava suficiente.

A expansão da internet, das redes sociais e das tecnologias digitais intensificou significativamente a coleta, o armazenamento e o compartilhamento de informações pessoais. Nesse cenário, os dados passaram a assumir relevante valor econômico e estratégico, constituindo importante ativo da economia orientada por dados (Pinheiro; Bonfim, 2022). Como consequência, ampliaram-se os riscos relacionados ao tratamento inadequado das informações, incluindo vazamentos, compartilhamentos indevidos e outras formas de violação aos direitos dos titulares.

À luz dessas considerações, o Brasil acompanhou o movimento internacional de fortalecimento da tutela informacional, fortemente influenciado pelo Regulamento Geral de Proteção de Dados da União Europeia (GDPR). Em resposta às novas demandas sociais, econômicas e tecnológicas, foi promulgada a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD). Para Doneda (2020), o regulamento europeu constituiu importante base para a elaboração da legislação brasileira, contribuindo para a construção de um modelo jurídico adequado aos desafios decorrentes da sociedade digital.

O artigo 1º da LGPD estabelece que a lei disciplina o tratamento de dados pessoais realizado por pessoas naturais e jurídicas, de direito público ou privado, com o objetivo de proteger a liberdade, a privacidade e o livre desenvolvimento da personalidade da pessoa natural (Brasil, 2018). Trata-se de diploma normativo de ampla incidência, cuja disciplina alcança praticamente toda atividade de tratamento de dados pessoais, independentemente do meio empregado, característica que confere à lei natureza transversal (Pinheiro; Bonfim, 2022).

A principal inovação da LGPD consistiu na instituição de um regime jurídico específico para disciplinar o tratamento de dados pessoais, estruturado a partir de fundamentos, princípios, direitos dos titulares e deveres atribuídos aos agentes de tratamento. Nesse sentido, Beltramini (2022) destaca que a lei estabeleceu a estrutura normativa necessária para o desenvolvimento de uma cultura de proteção de dados no ordenamento jurídico brasileiro. Esses elementos estruturantes serão examinados no tópico seguinte.

A LGPD não se limita a estabelecer regras procedimentais para o tratamento de dados pessoais. Antes de disciplinar direitos e obrigações, a lei estrutura um conjunto de fundamentos e princípios que orientam sua interpretação e aplicação, conferindo unidade e coerência ao sistema brasileiro de proteção de dados. Nesse sentido, Lemonje (2022) destaca que esses elementos desempenham papel essencial na organização e integração da disciplina jurídica da matéria.

Já o artigo 2º da LGPD estabelece os fundamentos que sustentam a disciplina do tratamento de dados pessoais. A proteção conferida pela lei não se restringe à preservação das informações, mas busca assegurar valores constitucionais como a privacidade, a liberdade, a autodeterminação informativa e o livre desenvolvimento da personalidade. Segundo Pinheiro e Bomfim (2022), esses fundamentos constituem parâmetros essenciais para a aplicação da legislação, orientando a tutela da dignidade da pessoa humana no ambiente digital.

Os fundamentos previstos na LGPD dialogam diretamente com a Constituição Federal e com o Código Civil, reforçando a proteção da privacidade, da intimidade e dos direitos da personalidade. Como destaca Doneda (2020), esses valores integram uma cláusula geral de tutela e promoção da pessoa humana, consolidando um modelo de proteção que coloca o titular dos dados no centro da disciplina jurídica.

Além dos fundamentos, a LGPD estabelece, em seu artigo 6º, um conjunto de princípios destinados a orientar todo o tratamento de dados pessoais. Esses princípios funcionam como parâmetros para a atuação dos agentes de tratamento e para a interpretação das disposições legais. Segundo Pinheiro e Bomfim (2022), eles desempenham função estruturante no sistema, orientando a aplicação das demais normas previstas na legislação.

Entre esses princípios, destacam-se a finalidade, a adequação e a necessidade, que constituem o núcleo de legitimação do tratamento de dados pessoais. Em conjunto, eles determinam que as informações sejam tratadas para finalidades legítimas, específicas e previamente informadas ao titular, limitando a coleta e a utilização dos dados ao mínimo necessário para a consecução desses objetivos. De acordo com Pinheiro e Bomfim (2022), o princípio da necessidade impõe a observância da proporcionalidade, vedando a coleta excessiva de informações.

A proteção conferida pela LGPD também se concretiza por meio dos princípios do livre acesso, da qualidade dos dados e da transparência. Esses

princípios asseguram ao titular o conhecimento sobre o tratamento de suas informações, bem como o acesso facilitado aos dados e a possibilidade de exigir sua atualização quando necessário. Segundo Martins (2022), tais mecanismos fortalecem o controle exercido pelo titular sobre o fluxo de seus dados pessoais.

Por sua vez, os princípios da segurança, da prevenção, da não discriminação e da responsabilização e prestação de contas impõem aos agentes de tratamento uma atuação preventiva e diligente na proteção das informações pessoais. Além da adoção de medidas técnicas e administrativas adequadas, exige-se a demonstração da efetividade dessas medidas. Nesse sentido, Zaffari e Limberger (2022) ressaltam que a LGPD consagra um modelo de atuação proativa, baseado na identificação, avaliação e mitigação contínua dos riscos decorrentes do tratamento de dados.

Nesse contexto, o artigo 5º da LGPD apresenta os conceitos essenciais para a aplicação da norma.

O artigo 5º, inciso I, da LGPD define dado pessoal como a “informação relacionada à pessoa natural identificada ou identificável” (Brasil, 2018).

De forma mais especifica, o dado pessoal sensível é definido no artigo 5°, inciso II:

> dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural; (Brasil, 2018).

Por fim, o tratamento é definido de forma ampla, no artigo 5°, inciso X:

> 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; (Brasil, 2018).

A lei também identifica os agentes responsáveis pelo tratamento de dados pessoais. Nos termos do artigo 5°, incisos VI e VII, respectivamente:

> VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
> VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador (Brasil, 2018).

Soma-se a essas figuras o encarregado, responsável por atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados, disposto no artigo 5°, inciso VIII (Brasil, 2018).

Conforme explica Comar (2022), esse agente exerce importante função de assessoramento ao controlador, contribuindo para a conformidade das atividades de tratamento com a legislação.

Para assegurar o exercício da autodeterminação informativa, a lei garante direitos como a confirmação da existência de tratamento, o acesso, a correção, a anonimização, a eliminação, a portabilidade dos dados, a revogação do consentimento e o acesso a informações sobre o tratamento realizado (Brasil, 2018). Nesse sentido, Marques e Lima (2022), destacam que a tutela jurídica da proteção de dados deve assegurar ao indivíduo o efetivo conhecimento e controle sobre o fluxo das informações que lhe dizem respeito.

A conjugação dos conceitos jurídicos, da definição dos agentes de tratamento e do catálogo de direitos assegurados aos titulares evidencia que a LGPD instituiu um sistema normativo completo para disciplinar o tratamento de dados pessoais. Como observa Beltramini (2022), esse modelo contribui para a consolidação de uma cultura de proteção de dados no Brasil. Todavia, quando o tratamento é realizado por órgãos e entidades estatais, a própria lei estabelece disciplina específica, em razão das peculiaridades inerentes à atuação da Administração Pública, tema que será abordado no tópico seguinte.

Nos termos dos artigos 23 e 24 da LGPD, o tratamento de dados pessoais pela Administração Pública deve estar vinculado à execução de políticas públicas, ao cumprimento de competências legais ou à prestação de serviços públicos (Brasil, 2018). Conforme observa Doneda (2020), a disciplina específica da lei reflete a necessidade de regulamentar o intenso fluxo informacional inerente às atividades estatais.

Embora disponha de prerrogativas legais para tratar dados pessoais, a Administração Pública permanece integralmente submetida aos princípios da LGPD, especialmente os da finalidade, necessidade, transparência e segurança (Brasil, 2018). Nesse sentido, Silva (2022) ressalta que a autorização legal para o tratamento de dados não confere ao Estado liberdade irrestrita para utilizar ou divulgar essas

informações, impondo-se a observância permanente dos direitos fundamentais dos titulares.

Além de estabelecer limites para o tratamento, a LGPD disciplina o compartilhamento de dados entre órgãos e entidades públicas, condicionando-o ao atendimento das finalidades legalmente previstas. A lei também impõe a adoção de medidas técnicas e administrativas destinadas a prevenir acessos não autorizados, perdas, alterações e vazamentos de informações. Conforme dispõe a própria LGPD (Brasil, 2018), tais medidas devem assegurar a proteção dos dados pessoais durante todo o ciclo de tratamento, inclusive após o seu encerramento, evidenciando a necessidade de uma governança permanente da informação.

Por outro lado, o art. 42 da Lei Geral de Proteção de Dados Pessoais atribui responsabilidade aos agentes de tratamento em situações que o dever de segurança não for cumprido:

> Art. 42. 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. (Brasil, 2018)

Assim, admite hipóteses de responsabilidade solidária quando o operador descumpre a legislação ou atua em desconformidade com as instruções lícitas do controlador, bem como quando houver mais de um controlador diretamente envolvido no tratamento do qual decorreram os danos (Brasil, 2018).

A efetividade desse regime jurídico, contudo, depende da existência de mecanismos institucionais capazes de orientar, fiscalizar e promover a correta aplicação da LGPD no âmbito da Administração Pública. Nesse cenário, Zandonai (2022) destaca que a existência de uma autoridade independente constitui elemento essencial para assegurar a implementação da legislação de proteção de dados. No ordenamento jurídico brasileiro, essa função é desempenhada pela Autoridade Nacional de Proteção de Dados.

3.2 Órgãos do Estado que protegem os Dados Pessoais

Uma vez delineadas as bases constitucionais e civis (jurídicas) da tutela de dados pessoais, cumpre identificar as instituições responsáveis por concretizar esse sistema no plano administrativo e jurisdicional. Nesse cenário, ANPD (Agência

Nacional de Proteção de Dados), Poder Judiciário e CNJ (Conselho Nacional de Justiça), desempenham funções complementares na fiscalização, regulamentação e tutela desse direito, especialmente diante da intensificação do tratamento estatal de dados.

3.2.1 Autoridade Nacional de Proteção de Dados (ANPD)

A Autoridade Nacional de Proteção de Dados (ANPD) ocupa posição central no sistema instituído pela LGPD, pois concentra funções de supervisão, regulação e fiscalização do tratamento de dados pessoais no Brasil. Sua relevância decorre da necessidade de mecanismos institucionais permanentes de controle em um ambiente marcado pelo tratamento massivo de informações e pelos riscos correspondentes (Doneda, 2020).

A ANPD foi instituída pela Lei nº 13.853, de 8 de julho de 2019, que promoveu alterações na Lei Geral de Proteção de Dados e inseriu dispositivos específicos destinados à criação da autoridade reguladora.

De acordo com o artigo 55-J da referida lei, compete à ANPD, entre outras atribuições, zelar pela proteção dos dados pessoais, fiscalizar o cumprimento da legislação, elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade, promover ações de conscientização e aplicar sanções administrativas em caso de descumprimento das normas legais.

A relevância institucional da ANPD decorre do reconhecimento da proteção de dados como direito fundamental pela Emenda Constitucional nº 115/2022, que introduziu o inciso LXXIX ao artigo 5º da Constituição Federal. A partir daí a atividade regulatória da autoridade passou a desempenhar papel essencial na concretização de um direito fundamental autônomo. Ainda assim, sua efetividade depende de capacidade institucional, coordenação com outros órgãos e produção de orientações claras para contextos públicos complexos, sob pena de se atribuir à autoridade protagonismo formal superior à sua capacidade prática de indução e fiscalização.

Entre as competências atribuídas à ANPD destaca-se a fiscalização de incidentes de segurança envolvendo dados pessoais. A LGPD dispõe, nos termos do artigo 46:

> Art. 46. 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.

. Quando ocorre incidente capaz de acarretar risco ou dano relevante aos titulares, a autoridade pode determinar providências específicas, exigir informações e acompanhar as medidas de mitigação adotadas.

A atuação da ANPD assume especial relevância quando o tratamento é realizado por órgãos e entidades da Administração Pública. Embora os artigos 23 a 32 da LGPD autorizem o Poder Público a tratar grandes volumes de informações para finalidades legítimas, esse tratamento permanece sujeito à fiscalização da autoridade nacional, especialmente em casos de incidentes de segurança ou potenciais violações aos direitos dos titulares.

Por essa razão, a importância da ANPD se projeta sobre a crescente digitalização dos serviços públicos e das bases estatais de dados. O tratamento de informações pessoais pelo Poder Judiciário e por sistemas vinculados ao CNJ permanece sujeito às diretrizes da LGPD e à supervisão institucional da autoridade. Essa constatação conduz, em seguida, ao exame do papel do próprio Poder Judiciário, simultaneamente guardião jurisdicional desse direito e agente de tratamento de grandes volumes de dados.

3.2.2 Poder Judiciário e o dever de proteção de dados pessoais

O Poder Judiciário desempenha papel essencial nessa matéria sob dupla perspectiva: assegura tutela jurisdicional aos titulares diante de lesões ou ameaças a seus direitos e, ao mesmo tempo, atua como agente de tratamento de grandes volumes de informações no próprio sistema de justiça. Essa dupla condição torna sua atuação especialmente relevante para a interpretação da LGPD, para a reparação de danos e para a observância de padrões rigorosos de segurança e governança.

A atuação do Poder Judiciário encontra fundamento no princípio da inafastabilidade da jurisdição, previsto no artigo 5º, inciso XXXV, da Constituição Federal, segundo o qual nenhuma lesão ou ameaça a direito pode ser excluída da apreciação judicial (Brasil, 1988). Em matéria de proteção de dados, esse princípio assegura aos titulares a possibilidade de buscar tutela jurisdicional sempre que houver violação de seus direitos decorrente do tratamento inadequado de informações pessoais.

Desta feita, a intervenção judicial torna-se particularmente relevante em situações de vazamentos, compartilhamentos indevidos, utilização abusiva de informações ou descumprimento das disposições previstas na Lei Geral de Proteção de Dados.

Sob a perspectiva constitucional, a atuação jurisdicional relaciona-se diretamente à proteção da dignidade da pessoa humana e dos direitos fundamentais. Como destaca Sarlet, esses direitos não apenas limitam o poder estatal, mas também compõem uma ordem objetiva de valores que orienta toda a atuação dos poderes públicos (Sarlet, 2021). Essa dimensão objetiva impõe ao Estado o dever de criar mecanismos aptos a assegurar sua efetividade, incluindo instrumentos jurisdicionais destinados à prevenção e reparação de lesões à esfera jurídica dos indivíduos.

Sob tal ótica, a digitalização das relações sociais e institucionais ampliou as demandas envolvendo privacidade, proteção de dados e segurança da informação. Ao mesmo tempo, a informatização do sistema de justiça formou extensas bases eletrônicas com dados processuais, administrativos e estatísticos, reforçando a necessidade de interpretação rigorosa da LGPD e de observância de padrões consistentes de segurança e governança. Essa duplicidade gera tensão institucional: o Judiciário controla a legalidade do tratamento realizado por terceiros enquanto precisa submeter suas próprias infraestruturas ao mesmo padrão de escrutínio.

Além da resolução de conflitos individuais, o Poder Judiciário exerce função relevante na tutela coletiva dos direitos relacionados à tutela de dados. Como muitos incidentes de segurança atingem simultaneamente grande número de titulares, as ações coletivas tornam-se instrumento importante para a proteção de interesses difusos e coletivos afetados por vazamentos ou outras violações informacionais, especialmente diante da assimetria informacional característica da sociedade contemporânea (Bioni, 2021).

No âmbito específico da Administração Pública, a atuação judicial assume especial relevância diante da crescente utilização de massivas bases de dados governamentais. Sistemas relacionados à saúde, previdência social, arrecadação tributária e atividade jurisdicional armazenam informações de elevada sensibilidade, cuja proteção constitui requisito indispensável para a preservação da confiança dos cidadãos nas instituições públicas (Doneda, 2020).

Nesse sentido, eventuais falhas na segurança dessas bases podem gerar controvérsias jurídicas envolvendo a observância dos deveres de proteção impostos

pela Constituição e pela LGPD, demandando a apreciação judicial acerca da compatibilidade da atuação estatal com os direitos fundamentais dos titulares. Como consequência, a relevância do Poder Judiciário também decorre da gestão de informações pelo próprio sistema de justiça. A transformação digital do setor resultou na criação de extensas bases eletrônicas destinadas ao armazenamento de informações processuais, administrativas e estatísticas, a exemplo da Base Nacional de Dados do Poder Judiciário - DataJud, instituída como fonte primária de dados do Sistema de Estatística do Poder Judiciário (Conselho Nacional De Justiça, 2020).

Embora tais sistemas contribuam para a eficiência e a transparência da atividade jurisdicional, também ampliam os desafios relacionados à segurança da informação e à tutela de dados pessoais, o que projeta especial destaque sobre a atuação do Conselho Nacional de Justiça, como se verá adiante.

3.2.3 Conselho Nacional de Justiça e a governança administrativa e tecnológica dos Tribunais

No âmbito da proteção de dados no Poder Judiciário, o Conselho Nacional de Justiça (CNJ) ocupa posição estratégica por coordenar a governança administrativa e tecnológica dos tribunais. Em um ambiente marcado pela informatização da justiça e pelo tratamento de dados processuais, cadastrais e sensíveis em larga escala, sua atuação é decisiva para transformar deveres constitucionais e legais de proteção em políticas concretas de segurança, conformidade e prevenção de incidentes. A informatização dos serviços jurisdicionais transformou o Poder Judiciário em relevante agente estatal de tratamento de dados pessoais em larga escala.

Com a entrada em vigor da LGPD, o tratamento de dados realizado por órgãos públicos passou a submeter-se explicitamente aos princípios da finalidade, adequação, necessidade, transparência e segurança (BRASIL, 2018).

Nesse cenário, destaca-se a Resolução CNJ nº 363, de 12 de janeiro de 2021, por meio da qual o Conselho Nacional de Justiça estabeleceu medidas para o processo de adequação dos tribunais à Lei Geral de Proteção de Dados Pessoais. A norma prevê diretrizes institucionais voltadas à implementação da LGPD no âmbito do Poder Judiciário, incluindo a criação de estruturas internas de governança, a definição

de responsabilidades e a adoção de providências destinadas à organização do tratamento de dados pessoais pelos tribunais (Conselho Nacional De Justiça, 2021a).

A resolução representa importante instrumento de concretização dos deveres legais de proteção, mas sua existência não assegura, por si só, implementação uniforme entre tribunais submetidos a diferentes condições estruturais, técnicas e orçamentárias. Por essa razão, a efetividade das medidas previstas depende de acompanhamento institucional contínuo, padronização mínima e mecanismos consistentes de verificação de conformidade, de modo a evitar que a adequação à LGPD permaneça restrita ao plano formal (Conselho Nacional De Justiça, 2021a).

Quando se trata de informações armazenadas em sistemas judiciais, os riscos da divulgação indevida são ainda mais sensíveis, pois os processos podem conter dados submetidos a sigilo legal ou judicial, especialmente nas hipóteses de segredo de justiça previstas e nas restrições de acesso aplicáveis aos documentos inseridos em processos eletrônicos. A análise desses deveres institucionais torna-se especialmente importante diante da possibilidade de vazamentos ou falhas de segurança em sistemas judiciais, circunstâncias que suscitam debates sobre a observância das exigências impostas pela Constituição e pela Lei Geral de Proteção de Dados.

3.3 Governança e Segurança da Informação no Poder Judiciário

A tutela de dados pessoais no âmbito do Poder Judiciário não depende apenas da observância das disposições da Lei Geral de Proteção de Dados Pessoais (LGPD), mas também da existência de estruturas organizacionais capazes de assegurar a proteção das informações sob custódia dos tribunais. Considerando que o sistema de justiça realiza diariamente o tratamento de grande volume de dados pessoais e sensíveis, incluindo informações processuais, cadastrais, biométricas e financeiras, a implementação de mecanismos permanentes de governança tornou-se requisito indispensável para a prevenção de incidentes e para a redução dos riscos associados ao ambiente digital (Doneda, 2020).

Sob essa perspectiva, o Conselho Nacional de Justiça passou a desempenhar papel central na construção de uma política institucional voltada à proteção de dados e à segurança cibernética. A atuação do órgão busca uniformizar

práticas entre os tribunais e estabelecer padrões mínimos de conformidade, reconhecendo que a proteção das informações não pode ser tratada como questão meramente tecnológica, mas como componente essencial da gestão pública e da própria atividade jurisdicional (CNJ, 2021a).

Um dos principais marcos normativos desse processo é a Resolução CNJ nº 363, de 2021, que estabeleceu medidas para a adequação dos tribunais à LGPD. O normativo determinou a adoção de programas de conformidade, a definição de responsabilidades institucionais relacionadas ao tratamento de dados pessoais e a implementação de mecanismos destinados à identificação e mitigação de riscos. A resolução também prevê a necessidade de mapeamento dos fluxos informacionais, elaboração de registros de tratamento e adoção de controles internos voltados à proteção dos direitos dos titulares (CNJ, 2021a).

A adequação promovida pela Resolução nº 363/2021 representa mudança relevante na forma como os órgãos judiciais administram informações pessoais. Essa tutela deixa de ser percebida apenas como obrigação legal e passa a integrar a estrutura de governança institucional dos tribunais, exigindo monitoramento contínuo e atuação preventiva. Paralelamente, a Resolução CNJ nº 396, de 2021, instituiu a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ). O ato normativo reconhece que a crescente dependência de sistemas eletrônicos amplia a exposição dos tribunais a ameaças digitais, exigindo medidas específicas para a proteção dos ativos informacionais e para a continuidade dos serviços jurisdicionais (CNJ, 2021b).

Nesse cenário, assume especial relevância a figura do encarregado pelo tratamento de dados pessoais (*Data Protection Officer* – DPO). Previsto no artigo 41 da LGPD, esse agente atua como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (Brasil, 2018). No âmbito do Poder Judiciário, a Resolução CNJ nº 363/2021 reforçou a necessidade de definição de responsáveis pela coordenação das ações relacionadas à proteção de dados, contribuindo para a institucionalização das práticas de conformidade e para a disseminação da cultura de proteção informacional (CNJ, 2021a).

Além das medidas preventivas, a estrutura de governança exige mecanismos eficazes de resposta a incidentes. Vazamentos de dados, ataques cibernéticos e acessos indevidos demandam atuação rápida por parte das instituições, tanto para reduzir os danos causados quanto para restabelecer a normalidade dos

sistemas afetados, especialmente diante dos deveres de segurança e comunicação previstos na LGPD (BRASIL, 2018).

Por essa razão, as diretrizes do CNJ estimulam a criação de protocolos formais de identificação, comunicação, tratamento e monitoramento de incidentes, permitindo respostas coordenadas em situações de crise no âmbito do Poder Judiciário (Conselho Nacional De Justiça, 2021b).

Esses procedimentos também contribuem para o cumprimento dos deveres de transparência previstos na LGPD. Quando o incidente for capaz de acarretar risco ou dano relevante aos titulares, o controlador deverá adotar as providências cabíveis para comunicação às autoridades competentes e aos próprios afetados, observando os parâmetros definidos pela legislação (Brasil, 2018).

Em síntese, a tutela de dados no Poder Judiciário passou a estruturar-se a partir de um modelo que combina conformidade normativa, gestão de riscos, segurança cibernética e responsabilização institucional. As Resoluções CNJ nº 363/2021 e nº 396/2021 representam marcos relevantes desse processo, ao estabelecerem parâmetros para a organização das práticas de proteção informacional no âmbito dos tribunais.

A consolidação dessas medidas assume especial importância diante da crescente digitalização da atividade jurisdicional e dos riscos associados à concentração de sistemas informacionais sob custódia do Estado. Mais do que garantir eficiência administrativa, esse modelo busca assegurar a proteção de direitos fundamentais e fortalecer a confiança social nas instituições responsáveis pela administração da justiça Mesmo diante de vários protocolos adotados, ainda é possível a ocorrência de vazamentos de dados em banco de dados de bases oficiais do Estado.

3.4 Análises de casos concretos envolvendo vazamentos de dados

Os vazamentos de dados pessoais exprimem os riscos inerentes ao tratamento massivo de informações na sociedade digital e, quando envolvem bases administradas pelo Poder Público, ganham relevo jurídico adicional por testarem a capacidade estatal de cumprir deveres de prevenção, segurança, governança e prestação de contas impostos pela Constituição e pela LGPD. Por isso, incidentes de segurança não constituem meras falhas técnicas: expõem titulares a vulnerabilidades

concretas e revelam se os agentes públicos adotaram medidas compatíveis com a sensibilidade das informações tratadas (Doneda, 2020; Bioni, 2021).

3.4.1 O Megavazamento de Dados de 2021

Os riscos inerentes ao tratamento massivo de dados tornaram-se particularmente visíveis no Brasil com o chamado megavazamento de 2021, episódio amplamente apontado como um dos maiores incidentes de exposição de dados pessoais já registrados no país (ANPD, 2021). O caso ganhou notoriedade após a divulgação de uma base com informações relativas a aproximadamente 223 milhões de pessoas físicas, número superior à população brasileira à época em razão da inclusão de registros de indivíduos falecidos (G1, 2021).

Entre os dados expostos encontravam-se informações cadastrais básicas, como nome completo, CPF, data de nascimento e endereço, além de elementos mais sensíveis relacionados à situação econômica dos titulares, incluindo renda presumida, score de crédito e outras informações utilizadas para fins de perfilização e análise de comportamento (ANPD, 2021).

O vazamento revelou a vulnerabilidade de grandes repositórios eletrônicos e demonstrou que a concentração de informações pessoais em ambientes digitais potencializa os impactos de falhas de segurança ou acessos não autorizados (Doneda, 2020). Embora a origem dos dados não tenha sido definitivamente esclarecida, o episódio desencadeou amplo debate sobre a efetividade dos mecanismos de proteção previstos na LGPD. A lei consagra, entre seus princípios, a segurança, a prevenção e a responsabilização dos agentes de tratamento, impondo a adoção de medidas técnicas e administrativas para proteger os dados contra acesso, perda, alteração, comunicação ou difusão indevida (Brasil, 2018).

Destarte, a dimensão do megavazamento evidenciou a relevância desses deveres e reforçou a necessidade de mecanismos permanentes de gestão de riscos por parte dos agentes responsáveis pelo tratamento das informações (Bioni, 2021). Sob a perspectiva dos titulares, os prejuízos decorrentes da exposição indevida de dados pessoais não se limitam aos aspectos patrimoniais. Conforme destaca Bioni (2021), a circulação descontrolada de informações pessoais pode comprometer a autonomia dos indivíduos, ampliar situações de vulnerabilidade e gerar impactos relevantes sobre o exercício da autodeterminação informativa.

A utilização indevida dos dados vazados pode favorecer a prática de fraudes eletrônicas, golpes financeiros, usurpação de identidade e outras condutas potencialmente lesivas aos direitos dos titulares.

Além disso, a exposição em larga escala compromete a confiança necessária ao funcionamento de relações sociais, econômicas e institucionais estruturadas sobre o tratamento de dados (Bioni, 2021). À luz dessas considerações, a tutela de dados transcende a esfera individual e também interessa à proteção de interesses difusos e coletivos, o que reforça a importância da atuação institucional na fiscalização das práticas de tratamento e na proteção dos titulares afetados (Sarlet, 2021).

Embora o megavazamento não tenha sido formalmente atribuído a um órgão público específico, o caso evidenciou que falhas na proteção de grandes bases informacionais produzem riscos sistêmicos incompatíveis com o padrão de tutela exigido pela Constituição e pela LGPD.

Sua principal implicação é jurídica, pois incidentes dessa magnitude reforçam que o dever estatal de proteção não se esgota na edição de normas, exigindo capacidade concreta de prevenção, resposta e governança. Quando o Estado detém ou coordena a custódia das informações afetadas, a inobservância desses deveres pode fundamentar o debate sobre responsabilidade civil, à luz da dimensão objetiva dos direitos fundamentais, dos deveres de segurança previstos na LGPD e do artigo 37, § 6º, da Constituição Federal (Sarlet, 2021).

O episódio também evidencia um problema metodológico relevante: mesmo quando a autoria do vazamento permanece incerta, a magnitude do dano social impõe a discussão de padrões objetivos de diligência na gestão de bases massivas, evitando que a indeterminação da origem do incidente neutralize o exame crítico das obrigações de segurança.

3.4.3 Vazamento de Dados Envolvendo Sistemas do Conselho Nacional de Justiça

Um dos episódios mais relevantes envolvendo proteção de dados no âmbito do Poder Judiciário ocorreu em 2025, quando o Conselho Nacional de Justiça (CNJ) comunicou incidente de segurança que resultou no acesso indevido a dados vinculados ao sistema de gerenciamento de chaves Pix. Segundo informações

divulgadas pelo próprio Conselho, foram afetados dados cadastrais associados a 11.003.398 pessoas, caracterizando um dos maiores incidentes de segurança já reportados por órgão integrante da estrutura do Poder Judiciário brasileiro (CNJ, 2025). Embora o CNJ tenha informado que não foram expostos dados sensíveis, senhas, saldos bancários ou informações protegidas por sigilo bancário, o episódio evidencia a dimensão dos riscos inerentes ao tratamento massivo de dados pessoais por instituições públicas.

A ocorrência demonstra que a mera exposição de informações cadastrais já possui potencial para gerar riscos aos titulares, especialmente quando consideradas práticas de engenharia social, fraudes eletrônicas e utilização indevida de dados para fins ilícitos (Bioni, 2021). A relevância jurídica do caso decorre não apenas da quantidade de pessoas atingidas, mas também da posição institucional ocupada pelo Conselho Nacional de Justiça. Como órgão responsável pela coordenação administrativa e pelo aperfeiçoamento da gestão do Poder Judiciário, o CNJ desempenha papel central na formulação de políticas de governança digital e proteção de dados. Em tal contexto, a ocorrência de incidente em sistema sob sua responsabilidade suscita reflexões acerca da efetividade das medidas de segurança adotadas e da capacidade institucional de prevenção de riscos informacionais.

Sob a perspectiva normativa, a situação deve ser analisada à luz do artigo 46 da Lei Geral de Proteção de Dados Pessoais, que impõe aos agentes de tratamento a obrigação de implementar medidas aptas a proteger os dados pessoais contra acessos não autorizados e situações acidentais ou ilícitas (Brasil, 2018).

Trata-se de dever jurídico de caráter permanente, cuja observância é exigida tanto de entidades privadas quanto de órgãos da Administração Pública. Além disso, o episódio reforça a importância dos princípios da prevenção e da responsabilização previstos nos incisos VIII e X do artigo 6º da LGPD.

Conforme observa Doneda (2020), a proteção informacional não se limita à reação posterior ao dano, exigindo dos agentes de tratamento uma postura preventiva baseada na identificação, avaliação e mitigação contínua dos riscos decorrentes do tratamento de informações pessoais.

No âmbito do Poder Judiciário, tais exigências foram incorporadas pela Resolução CNJ nº 363/2021, que instituiu diretrizes para a adequação dos tribunais à LGPD e estabeleceu mecanismos de governança voltados à proteção de dados pessoais. O incidente de 2025 demonstra que a existência de normas e estruturas

formais de conformidade não elimina a necessidade de constante aprimoramento das medidas de segurança cibernética, sobretudo em sistemas que concentram informações de milhões de cidadãos.

Sob o enfoque constitucional, a análise do caso ganha relevância adicional após a promulgação da Emenda Constitucional nº 115/2022, que elevou a tutela informacional à condição de direito fundamental autônomo. Dessa forma, falhas na segurança de sistemas públicos não representam apenas descumprimento de obrigações administrativas ou legais, mas podem configurar violações a direitos fundamentais relacionados à privacidade, à autodeterminação informativa e ao livre desenvolvimento da personalidade dos indivíduos afetados. Por fim, o incidente suscita debate acerca da responsabilidade civil estatal decorrente de falhas na proteção de dados pessoais.

Embora a configuração do dever de indenizar dependa da demonstração dos pressupostos jurídicos pertinentes, a ocorrência reforça a necessidade de examinar a aplicação conjunta do artigo 37, § 6º, da Constituição Federal e das disposições da LGPD relativas à responsabilização por danos causados em decorrência do tratamento inadequado de dados pessoais.

4 RESPONSABILIDADE CIVIL DO ESTADO POR VAZAMENTOS DE DADOS SIGILOSOS DE BANCO DE DADOS DO CNJ

A transformação digital promovida no âmbito do Poder Judiciário brasileiro modificou significativamente a forma como informações processuais e dados pessoais passaram a ser coletados, armazenados, compartilhados e utilizados pelos órgãos jurisdicionais. Nesse cenário, o Conselho Nacional de Justiça assumiu posição estratégica na coordenação de políticas nacionais voltadas à gestão de sistemas informatizados e bases de dados de alcance nacional, desempenhando papel essencial na modernização da prestação jurisdicional (Freitas; Chaves, 2022).

A expansão dessas atividades tornou ainda mais relevante a observância do direito fundamental à proteção de dados pessoais, reconhecido pelo Supremo Tribunal Federal (2020) como direito autônomo e posteriormente incorporado expressamente ao texto constitucional pela Emenda Constitucional nº 115/2022 (Brasil, 2022). Paralelamente, a Lei nº 13.709/2018 estabeleceu princípios, deveres e mecanismos destinados a assegurar que o tratamento de dados pessoais realizado pelo Poder Público ocorra em conformidade com os princípios da finalidade, necessidade, segurança, prevenção e responsabilização (Brasil, 2018).

A administração de extensas bases nacionais de dados judiciais faz com que o Conselho Nacional de Justiça atue como controlador (Brasil, 2018) de informações de elevada sensibilidade, reunindo registros processuais, criminais, familiares, patrimoniais e outros dados capazes de revelar aspectos relevantes da esfera privada dos jurisdicionados (Conselho Nacional de Justiça, 2021). Essa realidade amplia os riscos decorrentes de incidentes de segurança cibernética e evidencia a necessidade de adoção permanente de medidas técnicas e administrativas destinadas à prevenção de acessos indevidos, vazamentos e demais formas de tratamento incompatíveis com a legislação de proteção de dados.

Conforme observa Doneda (2020), a tutela jurídica dos dados pessoais está diretamente relacionada à proteção da dignidade da pessoa humana e ao exercício da autodeterminação informativa, enquanto Bioni (2021) destaca que a responsabilidade dos agentes de tratamento decorre da necessidade de assegurar confiança, transparência e segurança nas operações de tratamento de dados. Assim, eventual falha na proteção dessas informações pode gerar consequências jurídicas

relevantes, especialmente quanto à responsabilização civil do Estado pelos danos causados aos titulares.

Diante desse contexto, a presente seção examina o regime jurídico da responsabilidade civil aplicável ao Conselho Nacional de Justiça nos casos de vazamento de dados pessoais sigilosos sob sua administração. Para tanto, analisa-se inicialmente o enquadramento do CNJ como agente de tratamento de dados pessoais e o dever reforçado de proteção decorrente da natureza das informações administradas. Em seguida, são examinados o regime constitucional e legal da responsabilidade civil estatal, os pressupostos necessários à configuração do dever de indenizar.

Por fim, a aplicação dessas premissas ao dever de proteção de bancos de dados administrados pelo Conselho Nacional de Justiça, à luz da Constituição Federal, da Lei Geral de Proteção de Dados Pessoais, da doutrina especializada e da jurisprudência recente do Supremo Tribunal Federal e do Superior Tribunal de Justiça.

4.1 O CNJ como agente de tratamento de dados pessoais

A transformação digital do Poder Judiciário ampliou significativamente o tratamento de dados pessoais pelos órgãos judiciais. Nesse contexto, o Conselho Nacional de Justiça passou a coordenar e administrar bases nacionais de dados, concentrando informações essenciais ao funcionamento do sistema de justiça (Freitas; Chaves, 2022).

Como órgão integrante da Administração Pública, sua atuação submete-se à Lei Geral de Proteção de Dados Pessoais, especialmente quanto ao tratamento necessário ao atendimento de finalidade pública e ao cumprimento de competências legais, nos termos do art. 23 da Lei nº 13.709/2018:

> Art. 23. O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público (...).

Criado pela Emenda Constitucional nº 45/2004, o CNJ possui natureza constitucional e exerce papel relevante no planejamento e na implementação de políticas judiciárias nacionais (Freitas; Chaves, 2022). Suas competências encontram fundamento no art. 103-B, §4° da Constituição Federal, segundo o qual compete ao

Conselho “o controle da atuação administrativa e financeira do Poder Judiciário e do cumprimento dos deveres funcionais dos juízes” (Brasil, 1988).

A legitimidade desse modelo foi reconhecida pelo Supremo Tribunal Federal no julgamento da ADI nº 3.367/DF, no qual se assentou a constitucionalidade do Conselho Nacional de Justiça como órgão de natureza administrativa, incumbido do controle administrativo, financeiro e disciplinar do Poder Judiciário (Supremo Tribunal Federal, 2006).

A partir desse reconhecimento, o CNJ consolidou-se como instituição relevante para a coordenação de políticas nacionais voltadas à administração da Justiça (Freitas; Chaves, 2022).

Em razão de sua atuação executiva e coordenadora, o CNJ assumiu a administração de relevantes bancos de dados nacionais do Poder Judiciário, que serão analisados posteriormente.

A gestão dessas bases de dados envolve operações de tratamento de dados pessoais, nos termos do art. 5º, inciso X, da LGPD, razão pela qual o órgão deve observar as disposições aplicáveis ao Poder Público, especialmente quanto à finalidade pública, à segurança e à prevenção de incidentes (Brasil, 2018; Blum; López, 2020).

À luz do art. 5º, inciso VI, da LGPD:

> VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais; (Brasil, 2018

Assim, o CNJ enquadra-se como controlador, pois detém poder decisório sobre a organização, o compartilhamento e a gestão das bases nacionais sob sua administração, definindo finalidades e parâmetros do tratamento realizado (Freitas; Chaves, 2022). Essa incidência da LGPD foi reforçada pela Resolução CNJ nº 363/2021, que estabeleceu medidas para a adequação dos tribunais à legislação de proteção de dados (Conselho Nacional de Justiça, 2021).

Nos termos do artigo 46 da LGPD:

> 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 (Brasil, 2018).

Desta forma, na condição de controlador, o Conselho deve adotar medidas técnicas e administrativas aptas a proteger os dados pessoais sob sua guarda, prevenindo acessos não autorizados e situações acidentais ou ilícitas de destruição,

perda, alteração, comunicação ou tratamento inadequado (Superior Tribunal de Justiça, 2024).

4.2 Os bancos de dados do CNJ e o dever reforçado de proteção

Uma vez estabelecido que o Conselho Nacional de Justiça atua como controlador de dados pessoais, torna-se necessário examinar a natureza das informações tratadas em suas bases nacionais e o grau de proteção exigido para essas operações. Isto porque, ao administrar bases nacionais do Poder Judiciário, o CNJ concentra expressivo volume de informações dos cidadãos, o que amplia os riscos decorrentes de incidentes de segurança e impõe a observância de deveres de prevenção, segurança e vigilância (Freitas; Chaves, 2022).

Entre essas bases, destacam-se a Base Nacional de Dados do Poder Judiciário (DataJud), o Banco Nacional de Medidas Penais e Prisões (BNMP), o Sistema Nacional de Adoção e Acolhimento (SNA), os cadastros relativos a interceptações de comunicações e improbidade administrativa e a plataforma Codex, todos regulamentados por resoluções próprias.

A principal base nacional de dados administrada pelo Conselho Nacional de Justiça é a Base Nacional de Dados do Poder Judiciário (DataJud), instituída como fonte primária do Sistema de Estatística do Poder Judiciário (Conselho Nacional De Justiça, 2020).

O DataJud, instituído pela Resolução CNJ nº 331/2020 funciona como fonte primária do Sistema de Estatística do Poder Judiciário (CONSELHO NACIONAL DE JUSTIÇA, 2020). A plataforma centraliza dados e metadados processuais encaminhados pelos tribunais, favorecendo a produção de indicadores, a transparência e o planejamento de políticas judiciárias (Freitas; Chaves, 2022).

Essa base constitui relevante infraestrutura informacional do Poder Judiciário, reunindo dados processuais, criminais, cíveis, familiares e, em determinadas hipóteses, dados pessoais sensíveis dos jurisdicionados (Freitas; Chaves, 2022).

A centralização dessas informações em base nacional aumenta a extensão dos riscos, pois eventual acesso não autorizado ou vazamento pode comprometer simultaneamente dados pessoais de grande número de pessoas, exigindo padrões de segurança compatíveis com a natureza, a sensibilidade e a abrangência das informações administradas (Blum; López, 2020).

A relevância desse dever de proteção também decorre da natureza das informações armazenadas nos sistemas administrados pelo Conselho Nacional de Justiça. Além de dados de identificação civil, como nome, filiação, CPF, RG e endereço, essas bases podem reunir informações processuais, criminais e outros registros capazes de revelar aspectos da vida privada dos jurisdicionados (Freitas; Chaves, 2022).

A concentração dessas informações demonstra que os dados administrados pelo CNJ não constituem meros registros administrativos, mas elementos vinculados à privacidade, à autodeterminação informativa e aos direitos da personalidade dos titulares (Doneda, 2020). Assim, a proteção conferida pela LGPD não se limita à prevenção de acessos não autorizados, abrangendo também a adoção de medidas destinadas a evitar discriminação, vigilância indevida e utilização incompatível com a finalidade pública que justifica o tratamento (Blum; López, 2020).

A especial sensibilidade dessas informações impõe ao CNJ a observância dos deveres de segurança previstos na LGPD. Como observa Tasso (2020), a legislação atribui aos agentes de tratamento um dever permanente de prevenção e vigilância, cuja inobservância pode caracterizar falha na atividade de tratamento. Na mesma linha, Capanema (2020) destaca que a responsabilização do controlador pode decorrer tanto da violação dos princípios da LGPD quanto do descumprimento das medidas de segurança exigidas pelo ordenamento jurídico.

Esse dever de proteção também foi disciplinado internamente pelo Conselho Nacional de Justiça, por meio de sua Política de Segurança da Informação, que estabelece mecanismos de governança, gestão de riscos, controle de acesso aos sistemas e resposta a incidentes de segurança cibernética, com o objetivo de preservar a confidencialidade, a integridade e a disponibilidade das informações sob sua administração (Tasso, 2020). Tais diretrizes concretizam, no âmbito institucional, as exigências previstas na LGPD e reforçam a proteção dos dados pessoais como dever permanente da Administração Pública.

A relevância desse dever de proteção foi reconhecida pelo Supremo Tribunal Federal no julgamento da ADI nº 6.387. Esse julgamento marcou o reconhecimento, pelo STF, da proteção de dados pessoais como direito fundamental autônomo (Supremo Tribunal Federal, 2020).

Na ocasião Corte suspendeu a MP nº 954/2020, que previa o compartilhamento de dados de milhões de usuários de serviços de telecomunicações

com o IBGE, por ausência de finalidade específica e de garantias adequadas de segurança (Supremo Tribunal Federal, 2020). A decisão fortaleceu o princípio da autodeterminação informativa e contribuiu para a posterior inclusão expressa da proteção de dados na Constituição pela Emenda Constitucional nº 115/2022.

Nessa ocasião em que a Corte afirmou que o tratamento de dados pessoais deve observar os postulados da necessidade e da proporcionalidade, exigindo a adoção de 'mecanismos técnicos e administrativos aptos a proteger os dados pessoais de acessos não autorizados, vazamentos acidentais ou utilização indevida' (Supremo Tribunal Federal, 2020).

Assim, a implementação de medidas de segurança e governança não constitui mera opção administrativa, mas exigência decorrente da proteção constitucional dos dados pessoais e da disciplina estabelecida pela LGPD.

Aplicando essas premissas ao Conselho Nacional de Justiça, verifica-se que a proteção das bases nacionais sob sua administração constitui expressão concreta do direito fundamental à proteção de dados pessoais (Freitas; Chaves, 2022). Na condição de controlador de informações de elevada sensibilidade, incumbe ao órgão adotar medidas técnicas e administrativas compatíveis com os riscos da atividade, em conformidade com a LGPD e com sua Política de Segurança da Informação (Tasso, 2020).

A inobservância desses deveres pode caracterizar descumprimento das obrigações legais e regulamentares impostas ao controlador, especialmente quando evidenciada a ausência de mecanismos adequados de prevenção, gestão de riscos e proteção das informações sob sua responsabilidade. Tais falhas podem produzir consequências jurídicas relevantes, inclusive quanto ao dever de reparação dos danos eventualmente causados aos titulares das informações (Tasso, 2020).

Delineado o dever de segurança decorrente da administração de bases nacionais de elevada sensibilidade, passa-se ao exame do regime de responsabilidade civil do Estado aplicável aos incidentes envolvendo os bancos de dados administrados pelo CNJ.

4.3 O regime jurídico da responsabilidade civil do Estado sob a ótica da LGPD

Conforme demonstrado no tópico anterior, o Conselho Nacional de Justiça tem o dever jurídico de proteger os dados pessoais armazenados em suas bases

nacionais, exigência decorrente da Constituição Federal, da LGPD e das normativas internas do Poder Judiciário.

Todavia, a existência desse dever de prevenção e segurança não implica, por si só, responsabilidade automática em todo incidente cibernético. A obrigação de indenizar depende da presença dos requisitos definidos pelo ordenamento jurídico, razão pela qual se impõe delimitar o regime aplicável aos danos decorrentes de falhas na proteção dessas informações (Tasso, 2020).

A primeira matriz normativa encontra-se no art. 37, § 6º, da Constituição Federal, segundo o qual as pessoas jurídicas de direito público e as pessoas jurídicas de direito privado prestadoras de serviços públicos respondem pelos danos que seus agentes, nessa qualidade, causarem a terceiros (Brasil, 1988). O dispositivo consagra, como regra geral, a responsabilidade civil objetiva do Estado, fundada na teoria do risco administrativo, dispensando a comprovação de culpa e exigindo a demonstração da conduta estatal, do dano e do nexo de causalidade, sem prejuízo da análise de eventuais excludentes (Blum; López, 2020).

Esse modelo encontra fundamento nos princípios da igualdade e da repartição dos encargos sociais, pois os prejuízos anormais suportados individualmente por determinados administrados, quando decorrentes de atividade estatal exercida em benefício da coletividade, não devem recair exclusivamente sobre a vítima (Tasso, 2020). Aplicada ao tratamento de dados judiciais, essa lógica permite compreender que a manutenção de bases nacionais pelo Poder Público, embora necessária ao funcionamento do sistema de justiça, pode gerar riscos específicos aos titulares das informações.

Paralelamente à matriz constitucional, a Lei Geral de Proteção de Dados Pessoais instituiu disciplina específica de responsabilidade civil no artigo 42, prevendo o dever de reparação por danos patrimoniais, morais, individuais ou coletivos causados em razão de violação à legislação de proteção de dados (Brasil, 2018).

Desse modo, a responsabilidade civil por incidentes envolvendo dados pessoais administrados por órgão estatal deve ser compreendida a partir da articulação entre a Constituição Federal de 1988 e a LGPD. A Constituição estabelece o fundamento geral da responsabilidade civil do Estado, enquanto a LGPD especifica os deveres jurídicos aplicáveis ao tratamento de dados pessoais, especialmente os deveres de finalidade, prevenção, segurança e responsabilização (Blum; López,

2020). Não se trata, portanto, de regimes excludentes, mas de normas complementares na definição do dever de reparar.

No caso do Poder Público, essa integração normativa assume especial relevância. A LGPD alcança expressamente o tratamento de dados realizado pela Administração Pública, desde que vinculado ao atendimento de finalidade pública e ao cumprimento de competências legais (Brasil, 2018). Assim, o CNJ, ao administrar bases nacionais de dados judiciais, sujeita-se não apenas ao regime constitucional da responsabilidade civil estatal, mas também aos deveres específicos impostos aos agentes de tratamento pela legislação de proteção de dados (Blum; López, 2020).

A violação desses deveres pode caracterizar falha na atividade de tratamento e servir de fundamento para a responsabilização civil, desde que demonstrados os demais pressupostos necessários ao dever de indenizar (Tasso, 2020).

A natureza dessa responsabilidade, contudo, não é expressamente definida pela LGPD, o que gera debate doutrinário acerca da adoção de um modelo objetivo ou subjetivo no âmbito da proteção de dados (Blum; López, 2020).

Assim, o regime aplicável aos vazamentos de dados pessoais administrados pelo CNJ deve ser compreendido como integrado e complementar, pois a Constituição fornece o fundamento geral da responsabilidade estatal, enquanto a LGPD delimita os deveres específicos de proteção cuja violação pode ensejar o dever de reparação (Blum; López, 2020).

Em síntese, a responsabilidade civil decorrente de incidentes envolvendo dados pessoais administrados pelo Conselho Nacional de Justiça não se funda exclusivamente na Constituição Federal nem apenas na LGPD, mas sim na conjunção de ambos. Delimitado esse regime, passa-se à análise dos pressupostos necessários para a configuração do dever de indenizar nos casos de vazamento de dados pessoais.

4.3.1 Os pressupostos da responsabilidade civil do estado a partir da LGPD

Conforme assentado no tópico anterior, a responsabilidade civil aplicável à Administração Pública no tratamento de dados pessoais decorre da articulação entre a matriz constitucional e os deveres específicos previstos na LGPD (Blum; López, 2020). Todavia, a sujeição do ente estatal ao dever de segurança não implica

responsabilização automática em todo incidente cibernético, pois o direito brasileiro adota, como regra, a teoria do risco administrativo, e não a teoria do risco integral (Meirelles, 2016).

Para que surja o dever de indenizar, é necessária a presença dos pressupostos estruturais da responsabilidade civil: conduta estatal, dano e nexo de causalidade (Di Pietro, 2023). Assim, nos casos de vazamento de dados pessoais administrados pelo Conselho Nacional de Justiça, não basta a ocorrência material do incidente. É preciso demonstrar que o prejuízo suportado pelo titular decorreu de ação ou omissão imputável ao Poder Público, sem a incidência de causa capaz de romper o vínculo causal.

O primeiro pressuposto consiste na conduta estatal, que pode assumir natureza comissiva ou omissiva. No contexto do tratamento de dados pessoais, a conduta comissiva ocorre quando há tratamento ou compartilhamento irregular de informações (Tasso, 2020). Já a conduta omissiva manifesta-se quando o órgão deixa de observar as normas de prevenção e de segurança da informação, especialmente ao não adotar medidas técnicas para mitigar vulnerabilidades já conhecidas e documentadas (Capanema, 2020).

No caso do CNJ, a conduta relevante para fins de responsabilização deve ser analisada à luz dos deveres impostos aos agentes de tratamento, especialmente aqueles previstos no art. 46 da LGPD. Desse modo, a falha na gestão da segurança da informação, quando demonstrada, pode caracterizar descumprimento do dever legal de proteção e servir de fundamento para a responsabilidade civil do Estado (Blum; López, 2020).

O segundo pressuposto é a existência de dano. Conforme a doutrina administrativista, não há responsabilidade civil sem prejuízo efetivo à esfera juridicamente protegida de terceiro (Di Pietro, 2023). Por isso, a mera falha administrativa ou o simples descumprimento de norma de proteção de dados não bastam, isoladamente, para gerar reparação. É necessário que a conduta estatal produza consequência lesiva concreta, seja de natureza patrimonial, moral, individual ou coletiva.

Nos incidentes envolvendo dados pessoais, o dano pode assumir diferentes formas. Pode haver prejuízo material, quando a exposição das informações possibilita fraudes, perdas econômicas ou uso indevido de dados em prejuízo do titular. Também pode haver dano extrapatrimonial, especialmente quando o

vazamento compromete a privacidade, a intimidade, a autodeterminação informativa ou outros direitos da personalidade (Doneda, 2020). A gravidade do dano tende a se intensificar quando envolve dados sensíveis, informações criminais, familiares, processuais ou registros capazes de expor aspectos relevantes da vida privada dos jurisdicionados.

O terceiro pressuposto é o nexo de causalidade. Não basta que exista falha administrativa e prejuízo ao titular dos dados, é indispensável demonstrar que o dano decorreu diretamente da conduta estatal, seja ela comissiva ou omissiva (Tasso, 2020). Em outras palavras, a responsabilidade civil somente se configura quando a lesão sofrida pelo titular puder ser vinculada à atuação inadequada do Poder Público na gestão, proteção ou tratamento das informações.

Esse requisito assume especial relevância nos incidentes cibernéticos, pois a existência de ataque externo não afasta automaticamente a responsabilidade do agente de tratamento. Em tese, a atuação de terceiro pode romper o nexo causal, desde que o evento seja totalmente estranho à atividade estatal e não tenha sido favorecido por falha de segurança, ausência de controles adequados ou descumprimento de normas técnicas e jurídicas de proteção.

Segundo o entendimento jurisprudencial, em caso envolvendo uma ação movida por uma consumidora contra a concessionária de energia elétrica ENEL, motivada pelo vazamento de seus dados pessoais não sensíveis, como nome, CPF, RG, endereço e telefone, após um ataque hacker sofrido pela empresa, o vazamento de dados decorrente de falha de segurança caracteriza-se como 'fortuito interno', pois a proteção da informação é risco inerente e pressuposto da própria atividade de tratamento:

> O tratamento de dados pessoais configurou-se como irregular quando deixou de fornecer a segurança que o titular dele poderia esperar ("expectativa de legítima proteção"), consideradas as circunstâncias relevantes, entre as quais as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado (Superior Tribunal de Justiça, 2024).

Por outro lado, quando o vazamento ocorre em razão de vulnerabilidades conhecidas, deficiências de governança, falhas humanas evitáveis ou ausência de medidas compatíveis com os riscos da atividade, o ataque externo pode configurar fortuito interno, pois a segurança das bases de dados integra o próprio dever jurídico assumido pelo controlador (Superior Tribunal de Justiça, 2024). Nesses casos, não há

rompimento do nexo causal, uma vez que a omissão estatal contribui de forma direta para a concretização do dano.

Para afastar o dever de indenizar, é necessário verificar se, no caso concreto, foram implementadas medidas de segurança, prevenção e gestão de riscos compatíveis com a expectativa legítima de proteção do titular dos dados (Superior Tribunal de Justiça, 2024). Assim, a simples alegação de atuação criminosa de terceiro não basta para afastar a responsabilidade quando o incidente foi viabilizado por deficiência na proteção das informações.

Também devem ser consideradas as excludentes de responsabilidade admitidas pela teoria do risco administrativo. O Estado pode afastar o dever de indenizar quando demonstrar culpa exclusiva da vítima, fato exclusivo de terceiro, caso fortuito ou força maior, desde que tais circunstâncias rompam efetivamente o nexo causal (Meirelles, 2016). No campo da proteção de dados, isso significa que o CNJ não será responsabilizado quando comprovar que o dano decorreu de fator externo inevitável ou de conduta exclusiva do próprio titular, sem relação com falha de segurança, omissão administrativa ou inadequação das medidas de proteção adotadas.

A análise dos pressupostos da responsabilidade civil revela, portanto, que o dever de indenizar em casos de vazamento de dados pessoais sigilosos não decorre da simples ocorrência do incidente. Exige-se a demonstração de conduta imputável ao Estado, dano efetivo e nexo causal entre a falha e o prejuízo suportado pelo titular, além da ausência de causa excludente. Apenas quando esses elementos estiverem presentes será possível reconhecer a responsabilidade civil estatal pelos danos decorrentes de incidentes envolvendo dados pessoais.

4.4 Aplicação ao caso dos bancos de dados do CNJ

Aplicadas as premissas anteriores aos bancos de dados administrados pelo Conselho Nacional de Justiça, verifica-se que a responsabilidade civil do Estado por vazamento de dados pessoais sigilosos não decorre da simples ocorrência do incidente de segurança (Freitas; Chaves, 2022). Embora o CNJ se enquadre como controlador de dados pessoais e esteja submetido aos deveres previstos na LGPD, o dever de indenizar exige a demonstração de conduta imputável ao ente público, dano

efetivo e nexo causal entre a falha estatal e o prejuízo suportado pelo titular dos dados (Di Pietro, 2023).

No caso das bases nacionais sob gestão do CNJ, a conduta relevante pode consistir tanto em ato comissivo, como o tratamento inadequado, o compartilhamento irregular ou a permissão indevida de acesso às informações, quanto em omissão decorrente da ausência de medidas técnicas e administrativas adequadas à proteção dos dados (Tasso, 2020). Assim, o dever de reparação somente se configura quando o vazamento resultar de descumprimento dos deveres de segurança, prevenção e gestão de riscos impostos pela LGPD e pelas normas internas do Poder Judiciário (Superior Tribunal de Justiça, 2024).

A ocorrência de ataque externo, por si só, não afasta automaticamente a responsabilidade do agente de tratamento. Conforme reconhecido pelo Superior Tribunal de Justiça no REsp 2.147.374/SP, a incidência da excludente prevista no art. 43, III, da LGPD depende da verificação, no caso concreto, de que foram adotadas medidas técnicas e administrativas adequadas, acompanhadas de efetiva gestão de riscos e mecanismos de governança capazes de atender à legítima expectativa de proteção dos titulares (Superior Tribunal de Justiça, 2024). Desse modo, a alegação de culpa exclusiva de terceiro somente é admissível quando o incidente não tiver sido favorecido por falha de segurança ou descumprimento dos deveres legais de proteção.

Nessa linha, a doutrina destaca que a negligência do agente de tratamento pode ser caracterizada quando o vazamento decorre da inobservância de normas técnicas ou da manutenção de vulnerabilidades conhecidas e documentadas (Capanema, 2020). Por outro lado, a responsabilidade pode ser afastada quando demonstrado que o incidente resultou de evento inevitável, sem relação com falha do controlador, pois a obrigação de segurança prevista na LGPD possui natureza de obrigação de meio, e não de resultado (Capanema, 2020).

A sensibilidade das informações administradas pelo CNJ reforça a gravidade dos riscos envolvidos. Bases que reúnem dados processuais, criminais, familiares, patrimoniais ou informações referentes a crianças e adolescentes podem expor aspectos relevantes da vida privada dos jurisdicionados, ampliando a possibilidade de danos materiais, morais e discriminatórios em caso de vazamento (Supremo Tribunal Federal, 2020). Por essa razão, quanto maior a sensibilidade dos

dados tratados, maior deve ser o grau de diligência exigido do controlador na adoção de medidas de proteção compatíveis com os riscos da atividade.

Em resposta ao problema central da pesquisa, conclui-se que a responsabilidade civil do Estado por vazamentos de dados pessoais sigilosos administrados pelo Conselho Nacional de Justiça não é automática. Sua configuração exige a demonstração de conduta imputável ao ente estatal, dano e nexo causal, analisados à luz dos deveres específicos de proteção estabelecidos pela LGPD. Assim, comprovado que o vazamento decorreu da inobservância das medidas de segurança legalmente exigidas, e inexistindo causa excludente de responsabilidade, estará configurado o dever estatal de reparar os danos causados aos titulares dos dados.

5 CONSIDERAÇÕES FINAIS

A análise desenvolvida permitiu delimitar que a responsabilidade civil do Estado por incidentes de segurança envolvendo dados pessoais administrados pelo Conselho Nacional de Justiça não decorre automaticamente da simples ocorrência de vazamento, acesso indevido ou ataque cibernético. A responsabilização exige a verificação concreta de conduta imputável ao ente estatal, dano juridicamente relevante e nexo de causalidade entre a falha na proteção das informações e o prejuízo suportado pelo titular dos dados. O CNJ passou a ocupar posição central na circulação institucional de dados pessoais.

Ao coordenar políticas judiciárias e administrar repositórios nacionais, o órgão passou a lidar com informações que não se limitam a registros cadastrais ou processuais ordinários, alcançando dados capazes de revelar aspectos relevantes da vida privada dos jurisdicionados, inclusive em matéria criminal, familiar, patrimonial e envolvendo crianças e adolescentes. A responsabilidade civil decorrente de incidentes de segurança não pode ser examinada apenas a partir dos parâmetros tradicionais dos danos causados pela Administração Pública. A proteção de dados pessoais, após sua consolidação como direito fundamental, impõe que o tratamento estatal seja compreendido como atividade vinculada à preservação da privacidade, da autodeterminação informativa e dos direitos da personalidade.

A questão central não consistiu apenas em verificar se o CNJ pode ser responsabilizado por eventual vazamento, acesso indevido ou ataque cibernético, mas em identificar os pressupostos necessários para que um incidente de segurança gere dever estatal de indenizar. Essa delimitação evita tanto a transferência automática de todo risco tecnológico ao Estado quanto o afastamento da responsabilidade sempre que o evento lesivo envolver terceiros. O desenvolvimento

da pesquisa demonstrou que a responsabilidade civil do Estado, em matéria de proteção de dados, exige leitura integrada entre o regime constitucional de reparação, o sistema jurídico de proteção de dados pessoais e os deveres atribuídos ao controlador público.

A evolução histórica da responsabilidade estatal evidencia a superação da imunidade do poder público e a consolidação do dever de recompor danos injustamente suportados. No direito brasileiro, essa construção encontra núcleo no art. 37, § 6º, da Constituição Federal, que consagra a responsabilidade objetiva fundada no risco administrativo. Essa matriz constitucional deve ser lida em conjunto com a Constituição Federal, com o Código Civil e, de modo específico, com a Lei Geral de Proteção de Dados Pessoais. A LGPD impôs aos agentes de tratamento deveres de finalidade, adequação, necessidade, segurança, prevenção, responsabilização e prestação de contas. Esses parâmetros densificam a conduta exigida do ente público quando administra informações pessoais sob sua guarda.

A partir dessas premissas, verificou-se que o CNJ não atua como simples depositário técnico de informações. Ao definir finalidades, organizar sistemas, coordenar bases nacionais e editar normas internas de adequação e segurança, o órgão assume deveres próprios de governança informacional. A tutela dos dados pessoais, nesse contexto, alcança a atuação estatal e condiciona a legitimidade do tratamento realizado para finalidades públicas. A resposta ao problema de pesquisa conduz à conclusão de que a responsabilização civil do Estado por incidentes envolvendo dados pessoais administrados pelo Conselho Nacional de Justiça não decorre automaticamente da simples ocorrência de vazamento, acesso indevido ou ataque cibernético.

A existência do incidente, por si só, não basta para impor a obrigação indenizatória. É indispensável demonstrar conduta imputável ao Estado, dano juridicamente relevante e nexo de causalidade entre a falha estatal e o prejuízo suportado pelo titular. No caso do CNJ, a conduta pode manifestar-se de forma comissiva, quando houver tratamento inadequado, compartilhamento irregular ou utilização de informações em desconformidade com a finalidade pública que autorizou sua coleta. Também pode ocorrer por omissão, especialmente nos incidentes de segurança, quando se verificar a ausência ou insuficiência de medidas técnicas e administrativas exigidas pela LGPD e pelas normas internas de segurança da informação.

Essa distinção impede tanto a irresponsabilidade estatal quanto a adoção de uma responsabilidade integral não admitida como regra pelo ordenamento jurídico brasileiro. Nos atos comissivos, a matriz constitucional da responsabilidade objetiva possui especial incidência, desde que comprovados o dano e o nexo causal. Nos casos omissivos, ligados à falha de proteção, exige-se a demonstração de que o serviço não funcionou adequadamente ou deixou de observar os padrões de prevenção legalmente impostos.

A obrigação de segurança prevista na LGPD não corresponde a uma garantia absoluta de invulnerabilidade dos sistemas. Trata-se de dever jurídico de prevenção, que impõe atuação diligente, gestão de riscos, controle de acessos, resposta a incidentes e demonstração concreta de conformidade (BRASIL, 2018). Por isso, a culpa exclusiva de terceiro, o caso fortuito, a força maior ou a conduta exclusiva da vítima somente afastam a responsabilidade quando rompem o nexo causal e quando o evento não tiver sido favorecido por falha do serviço ou por deficiência de segurança.

Essas conclusões produzem consequências práticas relevantes para a Administração Pública e, de modo específico, para a gestão de dados no Poder Judiciário. O tratamento de informações pessoais pelo CNJ, embora voltado ao cumprimento de competências constitucionais e ao atendimento do interesse público, não se legitima apenas pela finalidade institucional que o justifica. A finalidade pública autoriza o tratamento, mas não afasta os direitos dos titulares nem reduz o cuidado exigido do controlador público.

A concentração nacional de dados processuais e pessoais exige padrões rigorosos de governança, pois eventual falha pode atingir simultaneamente grande número de pessoas e comprometer informações relacionadas à vida privada, à situação processual, à condição familiar, à liberdade e à identidade civil dos jurisdicionados. A Administração Pública deve, portanto, atuar de maneira preventiva, documentada e proporcional, restringindo acessos, mantendo sistemas seguros e demonstrando a efetividade das medidas adotadas.

A proteção de dados deixa de ser mero aspecto técnico da gestão administrativa e passa a integrar o conteúdo do dever estatal de tutela dos direitos fundamentais. A efetividade da privacidade e da autodeterminação informativa depende não apenas da reparação posterior ao dano, mas também da existência de mecanismos institucionais capazes de reduzir riscos antes que o incidente se

concretize. Quando esses mecanismos são negligenciados, a falha de segurança ultrapassa o plano operacional e assume relevância jurídica.

A contribuição da pesquisa reside em delimitar a responsabilidade civil do Estado nos incidentes de dados pessoais a partir de uma leitura integrada entre Direito Administrativo, direitos fundamentais e proteção de dados. Destarte, pôde-se concluir que não se mostra correto afirmar que todo vazamento em base pública gera, por si só, dever de indenizar. Também não se sustenta a tese de que ataques cibernéticos ou atos de terceiros afastam automaticamente a responsabilidade do controlador público.

O ponto decisivo está na verificação concreta da conduta estatal, do dano, do nexo causal e da observância dos deveres de segurança impostos ao agente de tratamento. No caso do Conselho Nacional de Justiça, a posição de controlador das bases nacionais administradas pelo órgão impõe padrão de diligência compatível com a natureza e a sensibilidade das informações sob sua guarda. Deste modo, a responsabilidade civil surge quando a exposição indevida dos dados decorre de falha imputável na estrutura de proteção, na governança, na prevenção ou na resposta a incidentes, desde que demonstrado prejuízo juridicamente reparável.

Conclui-se, portanto, que, nos incidentes envolvendo dados pessoais administrados pelo Conselho Nacional de Justiça, o dever de indenizar depende da comprovação de falha imputável ao ente estatal, de dano juridicamente relevante e de nexo causal entre a deficiência do serviço e a lesão sofrida. Essa conclusão harmoniza o regime constitucional da responsabilidade civil do Estado com os deveres específicos de proteção previstos na LGPD, assegurando tutela efetiva aos titulares sem afastar as causas excludentes admitidas pela teoria do risco administrativo.

REFERÊNCIAS

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **Comunicado sobre incidente de segurança envolvendo dados pessoais divulgado em janeiro de 2021**. Brasília: ANPD, 2021. Disponível em: https://www.gov.br/anpd. Acesso em: 13 jun. 2026.

MELLO, Celso Antônio Bandeira de. **Curso de direito administrativo**. 32. ed. São Paulo: Malheiros, 2015.

BELTRAMINI, Franciano. Dados pessoais: o que são? Quem os detém? Como e por que os coleta? In: BARZOTTO, Luciane Cardoso; COSTA, Ricardo Hofmeister de Almeida Martins (org.). **Estudos sobre LGPD: Lei Geral de Proteção de Dados – Lei nº 13.709/2018: doutrina e aplicabilidade no âmbito laboral**. Porto Alegre: Escola Judicial do Tribunal Regional do Trabalho da 4ª Região; Diadorim Editora, 2022.

BIONI, Bruno Ricardo. **Proteção de dados pessoais:** a função e os limites do consentimento. 3. ed. Rio de Janeiro: Forense, 2021.

BLUM, Renato Opice; LÓPEZ, Nuria. Lei Geral de Proteção de Dados no setor público: transparência e fortalecimento do Estado Democrático de Direito. **Cadernos Jurídicos**, São Paulo, ano 21, n. 53, p. 171-178, jan./mar. 2020.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 13 jun. 2026.

BRASIL. **Emenda Constitucional nº 115, de 10 de fevereiro de 2022**. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Brasília, DF: Congresso Nacional, 2022. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/emendas/emc/emc115.htm. Acesso em: 13 jun. 2026.

BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. **Código Civil**. Brasília, DF: Presidência da República, 2002. Disponível em:

https://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 13 jun. 2026.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 13 jun. 2026.

BRASIL. Lei nº 13.853, de 8 de julho de 2019. **Altera a Lei nº 13.709, de 14 de agosto de 2018**, para dispor sobre a proteção de dados pessoais e criar a Autoridade Nacional de Proteção de Dados. Brasília, DF: Presidência da República, 2019. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13853.htm. Acesso em: 13 jun. 2026.

CAPANEMA, Walter Aranha. A responsabilidade civil na Lei Geral de Proteção de Dados. **Cadernos Jurídicos**, São Paulo, ano 21, n. 53, p. 163-170, jan./mar. 2020.

COMAR, Rodrigo Thomazinho. Encarregado de dados – I. In: BARZOTTO, Luciane Cardoso; COSTA, Ricardo Hofmeister de Almeida Martins (org.). **Estudos sobre LGPD**. Porto Alegre: Escola Judicial do TRT da 4ª Região; Diadorim, 2022.

CONSELHO NACIONAL DE JUSTIÇA (Brasil). **Política de Segurança da Informação:** apresentação das diretrizes da Gestão de Segurança da Informação no ambiente do Judiciário. Brasília, DF, out. 2010.

CONSELHO NACIONAL DE JUSTIÇA (Brasil). **Resolução nº 331, de 20 de agosto de 2020**. Institui a Base Nacional de Dados do Poder Judiciário – DataJud. Brasília, DF: CNJ, 2020. Disponível em: https://atos.cnj.jus.br/atos/detalhar/3428.

CONSELHO NACIONAL DE JUSTIÇA (Brasil). **Resolução nº 363, de 12 de janeiro de 2021**. Estabelece medidas para o processo de adequação à Lei Geral de Proteção de Dados Pessoais a serem observadas pelos tribunais. Brasília: CNJ, 2021. Disponível em: https://atos.cnj.jus.br/atos/detalhar/3700. Acesso em: 13 jun. 2026.

CONSELHO NACIONAL DE JUSTIÇA (CNJ). **Resolução nº 396, de 7 de junho de 2021**. Institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ). Brasília: CNJ, 2021. Disponível em: https://atos.cnj.jus.br/atos/detalhar/3973. Acesso em: 13 jun. 2026.

CONSELHO NACIONAL DE JUSTIÇA (Brasil). **Resolução nº 446, de 14 de março de 2022**. Institui a plataforma Codex. Brasília, DF: CNJ, 2022. Disponível em: https://atos.cnj.jus.br/atos/detalhar/4417.

CONSELHO NACIONAL DE JUSTIÇA (CNJ). **Comunicado de incidente de segurança**. Brasília: CNJ, 2025. Disponível em: https://www.cnj.jus.br/comunicado-de-incidente-de-seguranca/. Acesso em: 13 jun. 2026.

CONSELHO NACIONAL DE JUSTIÇA (Brasil). **Resolução nº 289, de 14 de agosto de 2019**. Dispõe sobre a implantação e funcionamento do Sistema Nacional de Adoção e Acolhimento – SNA e dá outras providências. Diário da Justiça Eletrônico

do Conselho Nacional de Justiça, Brasília, DF, n. 165, p. 2-5, 15 ago. 2019. Disponível em: https://atos.cnj.jus.br/atos/detalhar/2976. Acesso em: 8 jul. 2026.

CONSELHO NACIONAL DE JUSTIÇA (Brasil). **Resolução nº 310, de 20 de março de 2020**. Altera as Resoluções CNJ nº 44, de 20 de novembro de 2007, e nº 59, de 9 de setembro de 2008, para atribuir a gestão dos bancos de dados do Cadastro Nacional de Condenados por Ato de Improbidade Administrativa e por Ato que Implique Inelegibilidade – CNCIAI e do Sistema Nacional de Controle de Interceptação – SNCI ao Comitê Gestor dos Cadastros Nacionais – CGCN. Diário da Justiça Eletrônico do Conselho Nacional de Justiça, Brasília, DF, n. 106, p. 2, 20 abr. 2020. Disponível em: https://atos.cnj.jus.br/atos/detalhar/3282. Acesso em: 8 jul. 2026.

CONSELHO NACIONAL DE JUSTIÇA (Brasil). **Resolução nº 417, de 20 de setembro de 2021**. Institui e regulamenta o Banco Nacional de Medidas Penais e Prisões – BNMP 3.0 e dá outras providências. Diário da Justiça Eletrônico do Conselho Nacional de Justiça, Brasília, DF, n. 244, p. 2-12, 21 set. 2021. Disponível em: https://atos.cnj.jus.br/atos/detalhar/4115. Acesso em: 8 jul. 2026.

SUPREMO TRIBUNAL FEDERAL (Brasil). **Ação Direta de Inconstitucionalidade nº 3.367/DF**. Relator: Ministro Cezar Peluso. Tribunal Pleno. Julgado em 13 abr. 2005. Publicado no Diário da Justiça em 17 mar. 2006. Disponível em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=2260590. Acesso em: 8 jul. 2026.

DI PIETRO, Maria Sylvia Zanella. **Direito administrativo**. 36. ed. Rio de Janeiro: Forense, 2023.

DONEDA, Danilo Cesar Maganhoto. **Da privacidade à proteção de dados pessoais: fundamentos da Lei Geral de Proteção de Dados**. 2. ed. São Paulo: Thomson Reuters Brasil, 2020.

FREITAS, Cláudio Delgado de; CHAVES, Luciano Athayde. **Base de Dados Nacional do Poder Judiciário e a Gestão dos Tribunais**. In: ENAJUS – Administration of Justice Meeting, 5., 2022, Curitiba. *Anais [...]* Curitiba: Universidade Positivo/UFRN, 2022.

G1. Megavazamento de dados de 223 milhões de brasileiros: o que se sabe e o que falta saber. G1, 28 jan. 2021. 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: 02. jul. 2026.

HOBBES, Thomas. **Leviatã**. São Paulo: Martins Fontes, 2003.

LEMONJE, Julise. Princípios na Lei Geral de Proteção de Dados Pessoais. In: BARZOTTO, Luciane Cardoso; COSTA, Ricardo Hofmeister de Almeida Martins (org.). **Estudos sobre LGPD**. Porto Alegre: Escola Judicial do TRT da 4ª Região; Diadorim, 2022.

LOCKE, John. **Segundo Tratado sobre o governo**. São Paulo: Martin Claret, 2006.

MARQUES, Claudia Lima; LIMA, Cíntia Rosa Pereira de. Relatório de impacto à proteção de dados dos trabalhadores. In: BARZOTTO; COSTA (org.). **Estudos sobre LGPD**. Porto Alegre: Escola Judicial do TRT da 4ª Região; Diadorim, 2022.

MARTINS, Renata Duval. Lei Geral de Proteção de Dados e princípio da proteção na relação laboral. In: BARZOTTO; COSTA (org.). **Estudos sobre LGPD**. Porto Alegre: Escola Judicial do TRT da 4ª Região; Diadorim, 2022.

MEIRELLES, Hely Lopes. **Direito administrativo brasileiro**. 42. ed. São Paulo: Malheiros, 2016.

PINHEIRO, Iuri; BOMFIM, Vólia. A Lei Geral de Proteção de Dados e seus impactos nas relações de trabalho. In: BARZOTTO; COSTA (org.). **Estudos sobre LGPD**. Porto Alegre: Escola Judicial do TRT da 4ª Região; Diadorim, 2022.

ROUSSEAU, Jean-Jacques. **O Contrato Social**. 4. ed. São Paulo: Martins Fontes, 2006.

SARLET, Ingo Wolfgang. **A eficácia dos direitos fundamentais**. 13. ed. Porto Alegre: Livraria do Advogado, 2021.

SILVA, Fabrício Lima. LGPD nas relações de trabalho. In: BARZOTTO; COSTA (org.). **Estudos sobre LGPD**. Porto Alegre: Escola Judicial do TRT da 4ª Região; Diadorim, 2022.

SUPERIOR TRIBUNAL DE JUSTIÇA (Brasil). **Recurso Especial nº 2.147.374/SP (2022/0220922-8)**. Relator: Ministro Ricardo Villas Bôas Cueva. Terceira Turma. Julgado em 3 dez. 2024. Publicado no DJEN/CNJ em 6 dez. 2024.

SUPREMO TRIBUNAL FEDERAL (Brasil). **Medida Cautelar na Ação Direta de Inconstitucionalidade nº 6.387/DF**. Relatora: Ministra Rosa Weber. Julgado em 24 abr. 2020. Publicado no DJe em 12 nov. 2020.

TASSO, Fernando Antonio. **A responsabilidade civil na Lei Geral de Proteção de Dados e sua interface com o Código Civil e o Código de Defesa do Consumidor**. Cadernos Jurídicos, São Paulo, ano 21, n. 53, p. 97-115, jan./mar. 2020.

ZAFFARI, Eduardo K.; LIMBERGER, Têmis. Rumo ao direito fundamental de proteção de dados pessoais. In: BARZOTTO; COSTA (org.). **Estudos sobre LGPD**. Porto Alegre: Escola Judicial do TRT da 4ª Região; Diadorim, 2022.

ZANDONAI, Camila Dozza. Autoridade Nacional de Proteção de Dados (art. 5º, XIX). In: BARZOTTO; COSTA (org.). **Estudos sobre LGPD**. Porto Alegre: Escola Judicial do TRT da 4ª Região; Diadorim, 2022.