A RESPONSABILIDADE CIVIL OBJETIVA DO ESTADO NO VAZAMENTO DE DADOS NO ÂMBITO DO PODER PÚBLICO

Alexandre Evangelista Silva Filho[1]

RESUMO: Este trabalho analisa a responsabilidade civil objetiva do Estado no vazamento de dados pessoais sob a guarda do Poder Público, com ênfase nas implicações jurídicas decorrentes da aplicação da teoria do risco administrativo. A crescente digitalização dos serviços estatais e o uso intensivo de dados pela Administração Pública impõem novos desafios à proteção da privacidade e à efetivação dos direitos fundamentais dos cidadãos. A partir de uma análise normativa da Constituição Federal, da Lei Geral de Proteção de Dados (Lei nº 13.709/2018 – LGPD), da Lei de Acesso à Informação (Lei nº 12.527/2011), do Código de Defesa do Consumidor e do Marco Civil da Internet, o estudo demonstra que o Estado brasileiro, na condição de controlador ou operador de dados, responde objetivamente por falhas na proteção da integridade, confidencialidade e disponibilidade dessas informações. A responsabilidade subsiste inclusive diante de ataques perpetrados por terceiros, como hackers, salvo comprovação inequívoca de excludentes legais. A jurisprudência dos tribunais superiores reforça a centralidade da responsabilidade objetiva estatal, evidenciando a obrigação de adoção de medidas preventivas e corretivas adequadas. O artigo sugere que o regime jurídico brasileiro privilegia uma lógica de justiça distributiva, em que o ônus das falhas sistêmicas na segurança informacional deve recair sobre o Estado.

Palavras-chave: Responsabilidade civil objetiva; Estado; vazamento de dados; LGPD; risco administrativo.

ABSTRACT: This article analyses the State's strict liability in cases of personal data breaches under the custody of public authorities, emphasizing the legal consequences arising from the application of the theory of administrative risk. The increasing digitalization of public services and the State's extensive use of personal data present new challenges to privacy protection and the enforcement of fundamental rights. Through a normative analysis of the Federal Constitution, the General Data Protection Law (Law No. 13,709/2018 – LGPD), the Access to Information Law (Law No. 12,527/2011), the Consumer Protection Code, and the Internet Civil Framework, this study demonstrates that the Brazilian State, acting as a data controller or processor, is strictly liable for failures in the protection of the integrity, confidentiality, and availability of personal information. This liability persists even in cases of third-party attacks, such as hacking incidents, unless there is clear evidence of legal exclusions. Case law from Brazil's higher courts supports the centrality of strict State liability and affirms the duty to adopt adequate preventive and reactive measures. The article suggests that Brazil's legal framework favors a distributive justice approach, whereby the burden of systemic failures in data security rightfully falls upon the State.

Keywords: Strict liability; State; data breach; LGPD; administrative risk.

1. INTRODUÇÃO

[1] Graduado em 2023 pela Faculdade de Direito da Universidade Federal da Bahia (UFBA), Especialista em Direito Processual Civil pela Faculdade de Minas (FACUMINAS).

A crescente transformação digital da Administração Pública tem ampliado significativamente o volume de dados pessoais tratados por órgãos e entidades estatais. Nesse cenário, a proteção das informações dos cidadãos deixa de ser apenas uma questão técnica e passa a configurar um imperativo jurídico e constitucional. A promulgação da Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e a inclusão do direito à proteção de dados como direito fundamental, por meio da Emenda Constitucional nº 115/2022, consolidaram a proteção de dados como um dos pilares do Estado Democrático de Direito no Brasil.

No desempenho de suas funções institucionais, o Estado atua como agente de tratamento de dados, sendo-lhe exigido o cumprimento de princípios como finalidade, necessidade, transparência e segurança. O eventual descumprimento desses deveres, mesmo que decorrente de ação de terceiros – como em casos de vazamentos causados por hackers –, pode ensejar a responsabilização civil do Estado. Essa responsabilidade, conforme dispõe o artigo 37, §6º da Constituição Federal, adota a forma objetiva quando relacionada à atuação da Administração Pública.

O presente trabalho tem como objetivo analisar a responsabilidade civil objetiva do Estado no vazamento de dados pessoais no setor público, à luz da teoria do risco administrativo. Com o fito de alcançar a análise desejada, examina-se a estrutura normativa vigente, os principais dispositivos legais aplicáveis e a evolução da jurisprudência dos tribunais superiores, buscando demonstrar que a responsabilização do Estado independe de culpa, desde que presente o nexo causal entre a atividade administrativa e o dano sofrido pelo titular dos dados. Trata-se, portanto, de compreender a responsabilidade estatal como expressão do dever de proteção e de garantia dos direitos fundamentais na sociedade informacional.

2. OS FUNDAMENTOS DA PROTEÇÃO DE DADOS NO SETOR PÚBLICO

A proteção de dados pessoais no âmbito do Poder Público constitui uma exigência constitucional central no regime do Estado Democrático de Direito, desdobrando-se a partir de uma malha normativa composta pela Constituição Federal, pela Lei nº 13.709/2018 (Lei Geral de Proteção de Dados – LGPD), pela Lei nº 12.527/2011 (Lei de Acesso à Informação – LAI), e, subsidiariamente, através de dispositivos do Código de Defesa do Consumidor (Lei nº 8.078/1990) e do Marco Civil

da Internet (Lei nº 12.965/2014). Esses diplomas normativos tratam do tema sob diferentes enfoques, mas convergem quanto à imposição de responsabilidades à Administração Pública pela guarda, tratamento e uso de dados pessoais.

A Constituição Federal de 1988, com a Emenda Constitucional nº 115/2022, introduziu o direito fundamental à proteção de dados pessoais no rol de direitos e garantias fundamentais do artigo 5º, inciso LXXIX, da CF/88, além de reconhecer a competência privativa da União para legislar sobre proteção de dados pessoais, vide art. 22, XXX, da CF/88, consolidando o papel da Lei Geral de Proteção de Dados (LGPD) como o marco regulatório da matéria.

No âmbito da LGPD, existem dispositivos normativos que estabelecem os deveres do Estado brasileiro enquanto agente de tratamento de dados. Por sua vez, o artigo 23, caput, incisos e parágrafos, disciplina que órgãos e entidades públicas estão sujeitos aos princípios da LGPD, devendo realizar o tratamento de dados para o cumprimento das atribuições do serviço público, porém, sob a condição de indicar um encarregado para o tratamento de dados pessoais e que sejam informadas as hipóteses em que são realizados os tratamentos de tais dados. Outrossim, o artigo 6º, caput e incisos, explicita os princípios aplicáveis, entre eles os da finalidade, necessidade, transparência e segurança. Já o artigo 44, caput e incisos, afirma que o tratamento será considerado irregular quando não observar a legislação de proteção de dados ou quando não fornecer a segurança que o titular pode esperar, o que impõe ao Poder Público a possibilidade de ser responsabilizado civilmente.

A responsabilidade civil pelo tratamento de dados pessoais está prevista no artigo 42, caput e parágrafos, da LGPD, haja vista que obriga o controlador ou operador que causar dano a terceiro, em decorrência de violação à legislação, a repará-lo. Embora o texto não mencione expressamente a culpa, os artigos 42 e 43, lidos em conjunto, indicam que o cumprimento da legislação pode excluir a responsabilidade. No entanto, conforme Isabella Laíse M. V. Vieira e Marcos Ehrhardt Junior (VIEIRA; EHRHARDT JUNIOR, 2024, p. 109), o art. 44, inciso II, da LGPD descreve que há a incidência da ideia de atividade de risco caracterizadora da teoria da responsabilidade civil objetiva ao fazer menção aos riscos que razoavelmente se esperam do tratamento de dados.

De acordo com Camila Ferrão dos Santos, Jeniffer Gomes da Silva e Vinicius Padrão (FERRÃO DOS SANTOS; GOMES DA SILVA; PADRÃO, 2021, p. 24), artigo 43 da LGPD estabelece que o agente de tratamento de dados só não será

responsabilizado em três situações específicas: quando não realizou o tratamento atribuído, quando, mesmo tendo realizado, não houve infração à legislação, ou quando o dano decorre exclusivamente de ação do titular ou de terceiros. Se não configurar um destes casos, a responsabilidade é presumida, independentemente de culpa. Essa estrutura normativa remete diretamente ao que prevê o artigo 12, §3º, do Código de Defesa do Consumidor, sugerindo que a LGPD adota um modelo de responsabilidade objetiva. A existência de um rol taxativo de excludentes reforça essa conclusão, já que, se a responsabilidade fosse subjetiva, bastaria ao agente provar a ausência de culpa, o que tornaria desnecessária essa delimitação legal.

Nesse sentido, nos casos em que a Administração Pública figura como agente de tratamento, faz-se mister a aplicação da teoria do risco administrativo, tornando a responsabilidade objetiva, conforme o artigo 37, §6º, da CF/88. A referida interpretação é reforçada pela Lei de Acesso à Informação (LAI) em seu artigo 31, pois estabelece que informações pessoais devem ser protegidas contra divulgação indevida, bem como o §2º prevê que aquele que der uso indevido a essas informações responderá pelos danos causados. Nesse ínterim, o artigo 34, caput, da LAI determina que os órgãos e entidades públicas respondem diretamente por danos decorrentes da divulgação não autorizada ou utilização indevida de dados pessoais, de modo que estes dispositivos não condicionam a responsabilização à demonstração de culpa, alinhando-se à lógica da responsabilidade objetiva.

Acerca da eventual sobreposição entre as normas supracitadas, a LGPD dispõe, em seu art. 52, §3º, acerca das sanções administrativas que os agentes de proteção de dados ficam sujeitos, permitindo a aplicação concomitante da LAI e da Lei de Improbidade Administrativa (Lei nº 8.429/92). Portanto, a disciplina da LAI subsiste no contexto da responsabilização estatal em razão de sua aderência à teoria do risco administrativo.

Segundo o entendimento pacificado do STJ (Brasil, Agravo Regimental no AREsp 354.991/RJ, 2013), a relação estabelecida entre a concessionária de serviço público e o consumidor final, no que diz respeito ao fornecimento de serviços públicos essenciais, como água e energia elétrica, é de natureza consumerista, o que permite a aplicação das normas previstas no Código de Defesa do Consumidor. Desse modo, o artigo 22, caput e incisos, do CDC estabelece que os órgãos públicos devem fornecer serviços adequados, eficientes, seguros e contínuos, e o seu artigo 14, caput,

impõe a responsabilização civil objetiva pelo defeito na prestação desses serviços, inclusive por falhas na proteção de dados.

Complementarmente, o Marco Civil da Internet, aplicável quando a Administração Pública atua por meio digital, reforça o dever estatal de garantir a segurança no armazenamento e tratamento de dados, nos termos dos artigos 10 e 11, caput e parágrafos. Tais normas exigem que a coleta e o uso das informações digitais pelo poder público sejam feitos com consentimento, finalidades legítimas e mecanismos robustos de proteção.

Portanto, sob a ótica do regime jurídico brasileiro, a proteção de dados no setor público envolve a conjugação de deveres de cautela, segurança e legalidade no tratamento de informações pessoais. O descumprimento desses deveres — mesmo que decorrente de omissões tecnológicas, falhas de governança ou ataques externos — não exclui, por si só, a responsabilidade do Estado. A legislação vigente atribui ao Poder Público o papel de garante da integridade e confidencialidade dos dados dos cidadãos, sendo seu dever estrutural assegurar medidas preventivas e reativas suficientes para evitar vazamentos e outras formas de tratamento indevido.

3. A RESPONSABILIDADE CIVIL OBJETIVA DO ESTADO E A TEORIA DO RISCO ADMINISTRATIVO NO VAZAMENTO DE DADOS POR HACKERS

Com base no entendimento de Hely Lopes Meirelles (Meirelles, 2016, p. 779), a responsabilidade civil do Estado, de natureza patrimonial, tem por objetivo a reparação dos danos causados e não se confunde com a responsabilidade penal ou administrativa, embora possa coexistir com estas. No âmbito da Administração Pública, essa responsabilidade impõe ao Estado o dever de indenizar terceiros pelos prejuízos decorrentes da atuação de seus agentes, ainda que esta ocorra sob o pretexto do exercício de suas funções, distinguindo-se da responsabilidade contratual ou legal.

Por sua vez, Maria Sylvia Zanella Di Pietro (DI PIETRO, 2023, p. 1651) define que a responsabilidade civil estatal possui natureza patrimonial e se fundamenta no artigo 186 do Código Civil, o qual consagra o princípio, amplamente aceito no ordenamento jurídico, de que aquele que causa dano a outrem deve repará-lo. A configuração do ilícito civil, conforme esse dispositivo, exige a presença de determinados elementos: uma conduta comissiva ou omissiva contrária ao direito; a

existência de culpa ou dolo — sendo que, diante da dificuldade de comprovação desse elemento subjetivo, o ordenamento admite, em hipóteses legais específicas, tanto a responsabilidade objetiva quanto a culpa presumida, que são exceções à regra geral da responsabilidade subjetiva; nexo de causalidade entre o comportamento e o dano; e a efetiva ocorrência de prejuízo, seja material ou moral.

Já Marçal Justen Filho (Justen Filho, 2023, p. 1473) propõe que a responsabilidade civil do Estado consiste na obrigação de reparar os prejuízos, tanto de ordem material quanto moral, experimentados por terceiros em decorrência de condutas comissivas ou omissivas ilícitas que possam ser atribuídas ao Poder Público. Tal obrigação inclui não somente os danos efetivamente causados, mas também os lucros cessantes, ou seja, aquilo que a vítima razoavelmente deixou de ganhar em razão do evento danoso imputável à atuação estatal.

Observa-se que a responsabilidade civil do Estado, possui natureza essencialmente patrimonial e decorre do dever estatal de reparar danos causados a terceiros, seja por ação direta ou por omissão. Embora o artigo 186 do Código Civil exija, como regra geral, a comprovação de dolo ou culpa para configuração do ilícito civil, admite-se a adoção da responsabilidade objetiva nos casos em que o risco da atividade estatal impõe à Administração o dever de indenizar independentemente da demonstração de culpa.

À medida em que se analisa a teoria do risco administrativo, sob a qual se aplica de maneira especial no contexto da proteção de dados pessoais em razão da assimetria informacional e a posição de vulnerabilidade do cidadão frente ao Estado, mesmo nos casos em que a violação de dados decorra de ação de terceiros — como em ataques cibernéticos — não se afasta, por si só, a responsabilidade estatal, uma vez que subsiste o dever de adoção de medidas adequadas de segurança e prevenção. A ausência ou insuficiência dessas medidas configura omissão relevante e enseja a responsabilidade civil do Poder Público, salvo comprovação inequívoca de causa excludente, o que é de difícil demonstração diante da previsibilidade de tais riscos no ambiente digital contemporâneo.

Para Hely Lopes Meirelles (Meirelles, 2016, p. 781-782), a teoria do risco administrativo funda-se na ideia de que, para que o Estado seja responsabilizado civilmente, basta a comprovação de um dano injusto decorrente da atuação administrativa, independentemente de qualquer demonstração de falha do serviço público ou de culpa dos agentes estatais. Diferente da teoria da culpa administrativa,

que exige a comprovação de uma omissão ou deficiência do serviço, o risco administrativo se estabelece apenas a partir do fato lesivo vinculado à atividade estatal. Logo, não se exige que a vítima comprove conduta culposa por parte do ente público, mas tão somente que demonstre o nexo entre o dano e a ação ou omissão do Estado. Essa teoria se fundamenta no princípio de que a atividade administrativa, ao gerar riscos à coletividade, pode impor prejuízos desiguais a determinados indivíduos, cabendo à coletividade, por meio do erário, compensar tais desigualdades. Diante do exposto, o risco da atividade e a solidariedade social constituem os pilares da doutrina, que visa realizar uma forma de justiça distributiva, sendo consagrada pelo ordenamento jurídico brasileiro. Importa destacar, contudo, que o risco administrativo não se confunde com o risco integral, pois admite a exclusão ou mitigação da responsabilidade estatal nos casos em que se comprove a culpa exclusiva ou concorrente da vítima pelo evento danoso.

Sob a visão de Marçal Justen Filho (Justen Filho, 2023, p. 1481-1482), cumpre distinguir a responsabilidade objetiva da responsabilidade por ato lícito atribuída ao Estado. A responsabilidade objetiva pressupõe a ocorrência de uma conduta estatal que, embora não dependa da comprovação de culpa, caracteriza violação à ordem jurídica. Por outro lado, há situações em que o Estado é chamado a indenizar danos causados a terceiros mesmo sem ter agido de forma ilícita ou reprovável, mas por ter gerado algum prejuízo ao jurisdicionado. Trata-se da chamada responsabilidade por ato lícito, ocorrendo quando os prejuízos são decorrentes de uma atuação legítima do Poder Público, mas que, ainda assim, geram efeitos adversos sobre indivíduos específicos. Em certos casos, a legislação pode impor ao Estado o dever de reparação mesmo na ausência de ilicitude, com base em fundamentos de equidade ou justiça compensatória.

Mediante as lições de Maria Sylvia Zanella Di Pietro (DI Pietro, 2023, p. 1763-1764), o Conselho de Estado francês, em determinadas circunstâncias, passou a adotar a teoria do risco como fundamento para a responsabilidade objetiva do Estado. Essa doutrina está alicerçada no princípio da igualdade de todos perante os encargos sociais, o qual tem origem no artigo 13 da Declaração dos Direitos do Homem de 1789. De acordo com esse princípio, os encargos decorrentes da atuação estatal devem ser distribuídos entre os cidadãos conforme suas possibilidades, de forma que, assim como os benefícios são compartilhados por todos, os danos sofridos por alguns membros da sociedade também devem ser repartidos. Quando um indivíduo arca com

um ônus desproporcional, desequilibrando a distribuição dos encargos sociais, o Estado tem o dever de reparar o prejuízo, utilizando os recursos públicos.

Ainda segundo a autora, nessa perspectiva, a ideia de culpa é substituída pelo nexo causal entre o funcionamento do serviço público e o dano experimentado pelo administrado. Independentemente de o serviço público ter sido prestado de maneira regular ou irregular, para que a responsabilidade objetiva seja configurada, são necessários três pressupostos: (a) a prática de um ato, lícito ou ilícito, por parte do agente público; (b) a ocorrência de um dano específico, que afeta um ou alguns membros da coletividade de maneira anormal, ou seja, que ultrapassa os inconvenientes habituais da convivência social; (c) a existência de um nexo causal entre o ato do agente público e o dano sofrido.

A responsabilidade civil do Estado pelo tratamento indevido ou pela exposição indevida de dados pessoais, ainda que resultante de ação de terceiros através de ataques cibernéticos, deve ser compreendida à luz da responsabilidade civil objetiva fundada na teoria do risco administrativo. No ordenamento jurídico brasileiro, tal teoria encontra respaldo no artigo 37, §6º, da Constituição Federal, bem como na Declaração dos Direitos do Homem de 1789 que fundamenta, no princípio da igualdade perante os encargos sociais, a reparação por danos anormais causados pela atividade estatal.

No contexto do tratamento de dados, a Lei Geral de Proteção de Dados (Lei nº 13.709/2018), em especial nos artigos 6º, 23, 42, 43 e 44, estabelece um regime de responsabilidade voltado à tutela da integridade informacional dos titulares, impondo deveres de segurança, transparência e finalidade ao Poder Público. A presença de um rol restrito de excludentes de responsabilidade, aliado à remissão aos riscos inerentes à atividade de tratamento, revela uma estrutura normativa afinada com a responsabilidade objetiva, corroborada por dispositivos da Lei de Acesso à Informação (Lei nº 12.527/2011, arts. 31 e 34), do Código de Defesa do Consumidor (Lei nº 8.078/1990, arts. 14 e 22) e do Marco Civil da Internet (Lei nº 12.965/2014, arts. 10 e 11).

A partir dessa moldura legal, desvela-se que o dever estatal de proteção de dados transcende o cumprimento meramente formal da legislação, configurando uma obrigação estruturante de natureza preventiva e reativa. A doutrina pátria aponta que, no âmbito da responsabilidade objetiva, o Estado pode ser compelido a indenizar se

houver nexo causal entre sua atuação (comissiva ou omissiva) e o dano específico e anormal sofrido por particulares, independentemente de demonstração de culpa.

O fundamento dessa responsabilização reside no risco que a própria atividade administrativa impõe ao cidadão — especialmente diante da assimetria informacional e da vulnerabilidade do indivíduo frente à máquina pública. Assim, mesmo em hipóteses de vazamento de dados causados por agentes externos, como hackers, subsiste o dever de responsabilização civil do Estado em casos que gerem prejuízos para os jurisdicionados, salvo demonstração inequívoca de culpa exclusiva da vítima, estado de necessidade, legítima defesa, exercício regular de direito e estrito cumprimento de dever legal, caso fortuito, força maior ou de fato de terceiro, hipóteses em que, à luz das exigências técnicas contemporâneas de segurança digital, revelam-se exceções e não a regra. Trata-se da consolidação de um regime de justiça distributiva aplicado à proteção de dados, em que o ônus decorrente da falha do sistema recai legitimamente sobre o Estado, sendo o Poder Público que detém o dever jurídico de assegurar a integridade e a confidencialidade das informações sob sua guarda.

4. A ANÁLISE JURISPRUDENCIAL DE PRECEDENTES DOS TRIBUNAIS SUPERIORES

No julgamento conjunto da ADI 6649/DF e da ADPF 695/DF, vide Informativo nº 1068, de relatoria do Ministro Gilmar Mendes, o Supremo Tribunal Federal reconheceu a constitucionalidade do compartilhamento de dados pessoais entre órgãos e entidades da administração pública federal, desde que este se realize em estrita observância aos princípios e salvaguardas previstos na Constituição Federal e na Lei Geral de Proteção de Dados Pessoais (LGPD). A Corte assentou que a proteção de dados e a autodeterminação informacional configuram direitos fundamentais autônomos, exigindo do Poder Público a adoção de parâmetros normativos e institucionais que assegurem a legalidade, necessidade, proporcionalidade e transparência no tratamento dessas informações. Com isso, o STF conferiu interpretação conforme à Constituição ao Decreto nº 10.046/2019, condicionando sua validade à aplicação compatível com os postulados da LGPD,

especialmente os princípios da finalidade, adequação e necessidade (art. 6º, incisos I a III), que regulam a atuação estatal em matéria de tratamento de dados.[2]

A decisão estabeleceu critérios rigorosos para a conformidade constitucional do compartilhamento, destacando-se a exigência de publicidade das hipóteses em que ocorre o tratamento de dados (art. 23, I, da LGPD), a limitação do acesso ao Cadastro Base do Cidadão a órgãos que comprovem finalidades legítimas e específicas, bem como a implementação de mecanismos de controle institucional pelo Comitê Central de Governança de Dados. A Corte determinou que tal Comitê deve garantir justificativa prévia e detalhada para a inclusão de novas bases temáticas ou atributos pessoais, observando os princípios da razoabilidade e proporcionalidade, e instituir sistemas de segurança e de rastreamento de acessos para fins de responsabilização. A responsabilização civil do Estado por eventuais violações à legislação de proteção de dados também foi expressamente reconhecida, nos termos dos arts. 42 e seguintes da LGPD, com possibilidade de ação regressiva contra o agente público infrator. Ademais, a omissão dolosa no dever de publicidade poderá configurar ato de improbidade administrativa, conforme art. 11, IV, da Lei nº 8.429/1992, reiterando o dever de transparência como elemento estruturante da atuação pública.[3]

Por fim, o STF modulou os efeitos da decisão, declarando com eficácia prospectiva a inconstitucionalidade do art. 22 do Decreto nº 10.046/2019, que previa a composição do Comitê Central de Governança de Dados exclusivamente por representantes do Poder Executivo. Concedeu-se prazo de 60 (sessenta) dias para que o Poder Executivo Federal reconfigure o Comitê, conferindo-lhe perfil institucional mais plural, técnico e independente, aberto à participação de outras instituições democráticas e dotado de garantias contra influências indevidas. Ao fazê-lo, a Corte não apenas reforçou o imperativo de compatibilização entre inovação tecnológica e

---

[2] BRASIL. *SUPREMO TRIBUNAL FEDERAL (STF)*. Ação Direta de Inconstitucionalidade n° 6.649 do Distrito Federal e Arguição de Descumprimento de Preceito Fundamental n° 695 do Distrito Federal. Informativo n° 1068 do STF. Relator Ministro Gilmar Mendes. Data do julgamento: 15/09/2022. Data de publicação: 23/09/2022. Disponível em: https://www.stf.jus.br/arquivo/informativo/documento/informativo1068.htm. Acesso em: 30 de abril de 2025.

[3] BRASIL. *SUPREMO TRIBUNAL FEDERAL (STF)*. Ação Direta de Inconstitucionalidade n° 6.649 do Distrito Federal e Arguição de Descumprimento de Preceito Fundamental n° 695 do Distrito Federal. Informativo n° 1068 do STF. Relator Ministro Gilmar Mendes. Data do julgamento: 15/09/2022. Data de publicação: 23/09/2022. Disponível em: https://www.stf.jus.br/arquivo/informativo/documento/informativo1068.htm. Acesso em: 30 de abril de 2025.

proteção de direitos fundamentais, como também afirmou a centralidade do controle público e da *accountability* na estrutura normativa de governança de dados, essencial para o desenvolvimento de políticas públicas em uma sociedade informacional regida pelos princípios do Estado Democrático de Direito.[4]

A análise do precedente supracitado corrobora a centralidade da responsabilidade estatal frente a falhas ou abusos no uso de dados pessoais. O STF destacou expressamente a possibilidade de responsabilização do Estado pelos danos decorrentes de violações à LGPD, inclusive com ação regressiva contra agentes públicos, o que reafirma a natureza objetiva dessa responsabilidade. Ademais, o descumprimento de deveres específicos, como o da publicidade e da limitação do tratamento ao mínimo necessário, destacou a possibilidade de responsabilização do agente estatal por improbidade administrativa em caso de transgressão dolosa por inobservância do dever de publicidade, ampliando a rede de sanções aplicáveis à má gestão de dados. Nesse contexto, o artigo 42 da LGPD e o artigo 11, IV, da Lei de Improbidade Administrativa se inserem como dispositivos operativos da tutela efetiva aos direitos dos titulares de dados, reforçando o entendimento de que o Estado não apenas responde pelos danos que causar, como também deve estruturar mecanismos internos de prevenção, controle e responsabilização.

Outrossim, o Superior Tribunal de Justiça, no julgamento do REsp nº 2.147.374-SP, vide Informativo nº 838, de relatoria do Ministro Ricardo Villas Bôas Cueva, reconheceu que reafirmou que as empresas que atuam como agentes de tratamento de dados, como a concessionária de energia elétrica ENEL, têm a responsabilidade legal de adotar medidas técnicas e administrativas adequadas para proteger os dados pessoais, conforme os princípios da Lei Geral de Proteção de Dados Pessoais (LGPD). Isso implica garantir que o tratamento de dados esteja em conformidade com a expectativa legítima de segurança e proteção dos titulares, considerando as tecnologias disponíveis. Quando essas medidas não são adotadas de forma eficaz, o tratamento é considerado irregular, colocando em risco a privacidade dos indivíduos.[5]

---

[4] BRASIL. *SUPREMO TRIBUNAL FEDERAL (STF)*. Ação Direta de Inconstitucionalidade n° 6.649 do Distrito Federal e Arguição de Descumprimento de Preceito Fundamental n° 695 do Distrito Federal. Informativo n° 1068 do STF. Relator Ministro Gilmar Mendes. Data do julgamento: 15/09/2022. Data de publicação: 23/09/2022. Disponível em: https://www.stf.jus.br/arquivo/informativo/documento/informativo1068.htm. Acesso em: 30 de abril de 2025.

[5] BRASIL. *SUPERIOR TRIBUNAL DE JUSTIÇA (STJ)*. REsp nº 2.147.374-SP. Informativo nº 838. Rel. Ministro RICARDO VILLAS BÔAS CUEVA, Terceira Turma, julgado em 03/12/2024, DJEN 06/12/2024. Disponível em:

No caso do REsp 2.147.374-SP, o STJ rejeitou a defesa da ENEL, que tentou se eximir de responsabilidade ao alegar que o vazamento de dados havia ocorrido exclusivamente por um ataque hacker. O tribunal deixou claro que a simples invocação de um evento externo não é suficiente para afastar a responsabilidade da empresa. Para isso, seria necessário comprovar que todas as medidas preventivas e mitigadoras haviam sido implementadas de maneira eficaz, reforçando o modelo de responsabilização proativa da LGPD. Esse entendimento amplia a responsabilidade das empresas em relação à proteção dos dados pessoais, mesmo que não haja evidência de danos morais.[6]

O julgado também destacou a força normativa da LGPD, que exige o cumprimento dos direitos dos titulares, apesar da ausência de danos morais. O STJ valorizou a transparência, a informação e o controle dos dados pessoais pelos titulares, aspectos essenciais da lei. A decisão reforçou o princípio da accountability, exigindo que o agente de tratamento atue com diligência, oferecendo provas concretas de que as medidas de segurança foram eficazes. Além disso, a empresa foi condenada a fornecer informações claras sobre o tratamento dos dados à titular, em conformidade com os artigos 18 e 19 da LGPD, ressaltando que a mera alegação de adoção de medidas de segurança não é suficiente para afastar a responsabilidade civil.[7]

O entendimento do STJ elucidado acima destaca que a responsabilidade civil objetiva do Estado, no contexto do tratamento de dados pessoais, pode ser vista como um reflexo do modelo de responsabilização proativa que vem sendo adotado pelo ordenamento jurídico brasileiro. Ao responsabilizar as instituições – seja na Administração pública direta e indireta, além das pessoas jurídicas de direito público ou privado – por falhas na proteção dos dados pessoais, a análise jurisprudencial do precedente do STJ reforça a ideia de que a responsabilização deve ocorrer

---

https://processo.stj.jus.br/jurisprudencia/externo/informativo/?acao=pesquisarumaedicao&livre=%270838%27.cod.. Acesso em: 30 de abril de 2025.

[6] BRASIL. *SUPERIOR TRIBUNAL DE JUSTIÇA (STJ)*. REsp nº 2.147.374-SP. Informativo nº 838. Rel. Ministro RICARDO VILLAS BÔAS CUEVA, Terceira Turma, julgado em 03/12/2024, DJEN 06/12/2024. Disponível em: https://processo.stj.jus.br/jurisprudencia/externo/informativo/?acao=pesquisarumaedicao&livre=%270838%27.cod.. Acesso em: 30 de abril de 2025.

[7] BRASIL. *SUPERIOR TRIBUNAL DE JUSTIÇA (STJ)*. REsp nº 2.147.374-SP. Informativo nº 838. Rel. Ministro RICARDO VILLAS BÔAS CUEVA, Terceira Turma, julgado em 03/12/2024, DJEN 06/12/2024. Disponível em: https://processo.stj.jus.br/jurisprudencia/externo/informativo/?acao=pesquisarumaedicao&livre=%270838%27.cod.. Acesso em: 30 de abril de 2025.

independentemente da ocorrência de culpa, desde que haja falha em adotar medidas adequadas de segurança. Por conseguinte, no âmbito do poder público, o Estado deve responder por danos decorrentes do vazamento de dados pessoais se for demonstrado que houve falha em suas políticas de segurança e na adoção de medidas técnicas e administrativas adequadas para proteger as informações dos cidadãos.

A correlação com a responsabilidade civil objetiva do Estado no vazamento de dados também se conecta com o julgamento do Supremo Tribunal Federal (STF) sobre o direito à proteção de dados pessoais como um direito fundamental, especialmente após a Emenda Constitucional 115/2022 que incluiu a proteção de dados pessoais como direito fundamental no artigo 5º da Constituição Federal. A decisão do STF estabelece que o poder público tem a obrigação de garantir a privacidade e a segurança dos dados pessoais, não apenas em termos de prevenção, assim como de resposta a incidentes a fim de garantir que os titulares dos dados possam obter a salvaguarda dos seus direitos de forma plena e transparente.

Todavia, a Segunda Turma do STJ, no julgamento do AREsp nº 2.130.619-SP, de relatoria do Ministro Francisco Falcão, concluiu que, em um caso envolvendo o vazamento de dados pessoais pela concessionária de energia elétrica, para que o vazamento de dados pessoais gere direito à indenização por dano moral, é necessário que o titular comprove efetivamente o dano sofrido, dado que o vazamento de dados pessoais "comuns" não é suficiente por si só para caracterizar o dano moral. A decisão reforça a ideia de que apenas dados sensíveis, conforme previstos na LGPD, gerariam dano moral presumido, como no caso de informações relacionadas à saúde, origem racial, convicções religiosas ou políticas, entre outros. Dessarte, a falha no tratamento de dados pessoais, embora indesejada, não resulta automaticamente em reparação financeira, o que exige um enfoque criterioso na aplicação da responsabilidade civil.[8]

Esta decisão do STJ, quando correlacionada ao tema da responsabilidade civil objetiva do Estado no vazamento de dados no âmbito público, define que o ente público gera dano moral presumido – *in re ipsa* – quando se trata de dados sensíveis. O vazamento de dados sensíveis de cidadãos, seja no âmbito privado ou público,

[8] BRASIL. *SUPERIOR TRIBUNAL DE JUSTIÇA (STJ)*. AREsp nº 2.130.619-SP. Rel. Ministro Francisco Falcão, Segunda Turma, julgado em 07/03/2023, DJEN 08/03/2023. Disponível em: https://processo.stj.jus.br/processo/julgamento/eletronico/documento/mediado/?documento_tipo=integra&documento_sequencial=178204788&registro_numero=202201522622&peticao_numero=&publicacao_data=20230310&formato=PDF. Acesso em: 30 de abril de 2025.

implica diretamente na violação de direitos fundamentais, exigindo a responsabilização objetiva, independentemente de culpa, como previsto pela LGPD. Não obstante, no direto difuso ou concreto, o arbitramento de danos morais à parte que tem seus dados invadidos por meio de hackers, em meio ao âmbito do Poder Público, está condicionado à demonstração de efetivo dano, como se demonstrou no caso acima acerca dos dados sensíveis previstos na LGPD.

5. CONCLUSÃO

A responsabilidade civil objetiva do Estado no tratamento inadequado ou no vazamento de dados pessoais, mesmo quando causado por terceiros, encontra sólido fundamento na Constituição Federal, na LGPD e na doutrina da teoria do risco administrativo. A análise empreendida ao longo deste trabalho evidenciou que o dever estatal de proteger os dados sob sua guarda ultrapassa a mera observância formal à legislação, configurando uma obrigação jurídica estrutural, voltada à prevenção e à reação eficaz diante de incidentes de segurança que possam gerar danos para os jurisdicionados.

A jurisprudência recente do Supremo Tribunal Federal e do Superior Tribunal de Justiça reafirma que a responsabilidade do Estado independe de culpa, desde que o dano seja decorrente de sua atividade administrativa e que haja o efetivo prejuízo sobre aqueles que sofrerem o vazamento de dados, ainda que haja envolvimento de agentes externos como hackers. Ressalvam-se apenas as hipóteses legalmente previstas de excludentes de responsabilidade, as quais demandam comprovação inequívoca.

Nesse sentido, o ordenamento jurídico brasileiro adota uma lógica de justiça distributiva, reconhecendo que os riscos inerentes à atividade estatal devem ser compensados por meio da responsabilização objetiva. A obrigação de indenizar decorre do princípio da solidariedade social, segundo o qual o cidadão não pode suportar sozinho os prejuízos resultantes de falhas no exercício da função administrativa.

Por conseguinte, para além da responsabilização exposta, o Estado deve estruturar políticas públicas eficazes de governança de dados, capacitar servidores, implementar medidas técnicas robustas e fortalecer mecanismos de auditoria e fiscalização. Somente assim será possível concretizar o direito fundamental à

proteção de dados e assegurar a confiança do cidadão na atuação da Administração Pública em um ambiente cada vez mais digital e vulnerável a riscos informacionais.

REFERÊNCIAS

BRASIL. *Constituição Federal de 1988*. Brasília. 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 30 abr. 2025.

BRASIL. *Decreto nº 10.046, de 9 de outubro de 2019*. Dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados. Brasília. 2019. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/d10046.htm. Acesso em: 30 abr. 2025.

BRASIL. *Emenda Constitucional nº 115/2022, de 10 de fevereiro de 2022*. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Brasília. 2022. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 30 abr. 2025.

BRASIL. *Lei nº 8.078, de 11 de setembro de 1990*. Dispõe sobre a proteção do consumidor e dá outras providências. Brasília. 1990. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 30 abr. 2025.

BRASIL. *Lei nº 8.429, de 2 de junho de 1992*. Dispõe sobre as sanções aplicáveis em virtude da prática de atos de improbidade administrativa, de que trata o § 4º do art. 37 da Constituição Federal; e dá outras providências. Brasília. 1990. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 30 abr. 2025.

BRASIL. *Lei nº 12.527, de 18 de novembro de 2011*. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Brasília. 2011. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 30 abr. 2025.

BRASIL. *Lei nº 12.965, de 23 de abril de 2014*. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília. 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 30 abr. 2025.

BRASIL. *Lei nº 13.709, de 14 de agosto de 2018*. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 30 abr. 2025.

BRASIL. *SUPERIOR TRIBUNAL DE JUSTIÇA (STJ)*. AREsp nº 2.130.619-SP. Rel. Ministro Francisco Falcão, Segunda Turma, julgado em 07/03/2023, DJEN 08/03/2023. Disponível em: https://processo.stj.jus.br/processo/julgamento/eletronico/documento/mediado/?documento_tipo=integra&documento_sequencial=178204788&registro_numero=202201522622&peticao_numero=&publicacao_data=20230310&formato=PDF. Acesso em: 30 abr. 2025.

BRASIL. *SUPERIOR TRIBUNAL DE JUSTIÇA (STJ)*. REsp nº 2.147.374-SP. Informativo nº 838. Rel. Ministro Ricardo Villas Bôas Cueva, Terceira Turma, julgado em 03/12/2024, DJEN 06/12/2024. Disponível em: https://processo.stj.jus.br/jurisprudencia/externo/informativo/?acao=pesquisarumaedicao&livre=%270838%27.cod.. Acesso em: 30 abr. 2025.

BRASIL. *SUPREMO TRIBUNAL FEDERAL (STF)*. Ação Direta de Inconstitucionalidade n° 6.649 do Distrito Federal e Arguição de Descumprimento de

Preceito Fundamental n° 695 do Distrito Federal. Informativo n° 1068. Relator Ministro Gilmar Mendes. Data do julgamento: 15/09/2022. Data de publicação: 23/09/2022. Disponível em: https://www.stf.jus.br/arquivo/informativo/documento/informativo1068.htm. Acesso em: 30 abr. 2025.

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

FERRÃO DOS SANTOS, Camila; GOMES DA SILVA, Jeniffer; PADRÃO, Vinicius. *Responsabilidade civil pelo tratamento de dados pessoais na Lei Geral de Proteção de Dados.* Vol. 4. Ed. 3. Revista Eletrônica Da PGE-RJ, 2021. Disponível em: https://revistaeletronica.pge.rj.gov.br/index.php/pge/article/view/256. Acesso em: 30 abr. 2025.

JUSTEN FILHO, Marçal. Curso de *Direito Administrativo*. 14ª ed. Rio de Janeiro: Editora Forense, 2023.

MEIRELLES, Hely Lopes. *Direito Administrativo Brasileiro*. Atualizada por José Emmanuel Burle Filho e Carla Rosado Burle. 42ª ed. São Paulo: Editora Malheiros, 2016.

VIEIRA, Isabella Laíse M. V.; Ehrhardt Junior, Marcos. *COMO A LGPD DISCIPLINA A RESPONSABILIDADE CIVIL NAS OPERAÇÕES DE TRATAMENTO DE DADOS PESSOAIS?* Vol. 16. Ed. 39. Revista Duc In Altum - Cadernos De Direito, Faculdade Damas, 2024. Disponível em: https://revistas.faculdadedamas.edu.br/index.php/cihjur/article/view/3012. Acesso em: 30 abr. 2025.