SUPERIOR TRIBUNAL DE JUSTIÇA

RECURSO ESPECIAL Nº 2147374 - SP (2022/0220922-8)

RELATOR	**:**	**MINISTRO RICARDO VILLAS BÔAS CUEVA**
RECORRENTE	:	ELETROPAULO METROPOLITANA ELETRICIDADE DE SAO PAULO S.A.
ADVOGADO	:	GUSTAVO ANTONIO FERES PAIXAO - SP186458A
RECORRIDO	:	THAYNA NAYARA DA SILVA QUEIROZ
ADVOGADO	:	ADILSON ALMEIDA DE VASCONCELOS - SP146989
INTERES.	:	ENEL DISTRIBUIÇÃO SAO PAULO S/A
ADVOGADO	:	GUSTAVO ANTONIO FERES PAIXAO - SP186458

EMENTA

RECURSO ESPECIAL. LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS. DIREITO À PRIVACIDADE, À LIBERDADE E À AUTODETERMINAÇÃO INFORMATIVA. AGENTE DE TRATAMENTO. VAZAMENTO DE DADOS NÃO SENSÍVEIS DO TITULAR. INCIDENTE DE SEGURANÇA. ATAQUE HACKER. RESPONSABILIDADE EXCLUSIVA DE TERCEIRO. NÃO COMPROVADA. RESPONSABILIDADE CIVIL PROATIVA. EXPECTATIVA DE LEGÍTIMA PROTEÇÃO. COMPLIANCE E REGULAÇÃO DE RISCO DA ATIVIDADE. DIREITOS DO TITULAR. CONCRETIZAÇÃO. APLICABILIDADE.

1. A controvérsia jurídica consiste em definir se o vazamento de dados pessoais não sensíveis do titular, decorrente de atividade alegadamente ilícita, é passível de imputar ao agente de tratamento de dados as obrigações previstas no art. 19, II, da LGPD, ou se o fato de tal vazamento ter decorrido de atividade ilícita seria uma excludente de responsabilidade, prevista no art. 43, III, da LGPD.

2. Ao inscrever a proteção e o tratamento de dados pessoais no rol dos direitos e garantias fundamentais da Constituição (art. 5º, LXXIX), a Emenda Constitucional nº 115/2022 inaugurou um novo capítulo no ordenamento jurídico brasileiro no que tange aos direitos de personalidade, à liberdade e à autodeterminação informativa.

3. A empresa recorrente, pelo fato de se enquadrar na categoria dos agentes de tratamento, tinha a obrigação legal de tomar todas as medidas de segurança esperadas pelo titular para que suas informações fossem protegidas, e seus sistemas utilizados para o tratamento de dados pessoais deveriam estar estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos na LGPD e às demais normas regulamentares.

4. *Compliance* de dados é o esforço de conformidade e de aplicação da LGPD nas atividades das empresas que lidam com tratamento de dados. Referido instrumento assume importância central ao induzir não apenas à obediência ao direito, mas também à comprovação da efetividade dos programas de conformidade.

5. 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 (art. 44, III, da LGPD).

6. Ao não provar, perante as instâncias ordinárias, que o vazamento dos

dados da recorrida teria se dado exclusivamente em razão do incidente de segurança, é impossível aplicar em favor da recorrente a excludente de responsabilidade do art. 43, III, da LGPD.

7. Assim, correta a conclusão do TJSP de concretizar os direitos do titular ao condenar a recorrente na obrigação de apresentar informação das entidades públicas e privadas com as quais realizou o uso compartilhado dos dados da recorrida (art. 18, VII, da LGPD) e a fornecer declaração completa que indique a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, bem como a cópia exata de todos os dados referentes ao titular constantes em seus bancos de dados (art. 19, II, da LGPD).

8. Recurso especial não provido.

ACÓRDÃO

Vistos e relatados estes autos em que são partes as acima indicadas, acordam os Ministros da TERCEIRA TURMA, por unanimidade, negar provimento ao recurso especial, nos termos do voto do Sr. Ministro Relator.

Os Srs. Ministros Nancy Andrighi, Humberto Martins e Moura Ribeiro votaram com o Sr. Ministro Relator.

Presidiu o julgamento o Sr. Ministro Humberto Martins.

Brasília, 04 de dezembro de 2024.

Ministro RICARDO VILLAS BÔAS CUEVA
Relator

Documento eletrônico VDA44763188 assinado eletronicamente nos termos do Art.1º §2º inciso III da Lei 11.419/2006
Signatário(a): RICARDO VILLAS BÔAS CUEVA Assinado em: 04/12/2024 16:07:38
Publicação no DJEN/CNJ de 06/12/2024. Código de Controle do Documento: e2153341-c7f8-4f88-91da-fc09b566f215

SUPERIOR TRIBUNAL DE JUSTIÇA

RECURSO ESPECIAL Nº 2147374 - SP (2022/0220922-8)

RELATOR	**:**	**MINISTRO RICARDO VILLAS BÔAS CUEVA**
RECORRENTE	:	ELETROPAULO METROPOLITANA ELETRICIDADE DE SAO PAULO S.A.
ADVOGADO	:	GUSTAVO ANTONIO FERES PAIXAO - SP186458A
RECORRIDO	:	THAYNA NAYARA DA SILVA QUEIROZ
ADVOGADO	:	ADILSON ALMEIDA DE VASCONCELOS - SP146989
INTERES.	:	ENEL DISTRIBUIÇÃO SAO PAULO S/A
ADVOGADO	:	GUSTAVO ANTONIO FERES PAIXAO - SP186458

EMENTA

RECURSO ESPECIAL. LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS. DIREITO À PRIVACIDADE, À LIBERDADE E À AUTODETERMINAÇÃO INFORMATIVA. AGENTE DE TRATAMENTO. VAZAMENTO DE DADOS NÃO SENSÍVEIS DO TITULAR. INCIDENTE DE SEGURANÇA. ATAQUE HACKER. RESPONSABILIDADE EXCLUSIVA DE TERCEIRO. NÃO COMPROVADA. RESPONSABILIDADE CIVIL PROATIVA. EXPECTATIVA DE LEGÍTIMA PROTEÇÃO. COMPLIANCE E REGULAÇÃO DE RISCO DA ATIVIDADE. DIREITOS DO TITULAR. CONCRETIZAÇÃO. APLICABILIDADE.

1. A controvérsia jurídica consiste em definir se o vazamento de dados pessoais não sensíveis do titular, decorrente de atividade alegadamente ilícita, é passível de imputar ao agente de tratamento de dados as obrigações previstas no art. 19, II, da LGPD, ou se o fato de tal vazamento ter decorrido de atividade ilícita seria uma excludente de responsabilidade, prevista no art. 43, III, da LGPD.

2. Ao inscrever a proteção e o tratamento de dados pessoais no rol dos direitos e garantias fundamentais da Constituição (art. 5º, LXXIX), a Emenda Constitucional nº 115/2022 inaugurou um novo capítulo no ordenamento jurídico brasileiro no que tange aos direitos de personalidade, à liberdade e à autodeterminação informativa.

3. A empresa recorrente, pelo fato de se enquadrar na categoria dos agentes de tratamento, tinha a obrigação legal de tomar todas as medidas de segurança esperadas pelo titular para que suas informações fossem protegidas, e seus sistemas utilizados para o tratamento de dados pessoais deveriam estar estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos na LGPD e às demais normas regulamentares.

4. *Compliance* de dados é o esforço de conformidade e de aplicação da LGPD nas atividades das empresas que lidam com tratamento de dados. Referido instrumento assume importância central ao induzir não apenas à obediência ao direito, mas também à comprovação da efetividade dos programas de conformidade.

5. 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 (art. 44, III, da LGPD).

6. Ao não provar, perante as instâncias ordinárias, que o vazamento dos

dados da recorrida teria se dado exclusivamente em razão do incidente de segurança, é impossível aplicar em favor da recorrente a excludente de responsabilidade do art. 43, III, da LGPD.
7. Assim, correta a conclusão do TJSP de concretizar os direitos do titular ao condenar a recorrente na obrigação de apresentar informação das entidades públicas e privadas com as quais realizou o uso compartilhado dos dados da recorrida (art. 18, VII, da LGPD) e a fornecer declaração completa que indique a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, bem como a cópia exata de todos os dados referentes ao titular constantes em seus bancos de dados (art. 19, II, da LGPD).
8. Recurso especial não provido.

RELATÓRIO

Trata-se de recurso especial, com fundamento no art. 105, III, "a", da Constituição Federal, interposto por ELETROPAULO METROPOLITANA ELETRICIDADE DE SÃO PAULO S.A. ("ENEL"), contra o acórdão do Tribunal de Justiça do Estado de São Paulo assim ementado:

> *"LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD) E DIREITO DO CONSUMIDOR. AÇÃO COM PRECEITOS CONDENATÓRIOS. Sentença de improcedência dos pedidos. Recurso de apelação da autora. Vazamento de pessoais não sensíveis da autora (nome completo, números de RG e CPF, endereço, endereço de e-mail e telefone), sob responsabilidade da ré. LGPD. Responsabilidade civil ativa ou proativa. Doutrina. Código de Defesa do Consumidor. Responsabilidade civil objetiva. Ausência de provas, todavia, de violação à dignidade humana da autora e seus substratos, isto é, liberdade, igualdade, solidariedade e integridade psicofísica. Autora que não demonstrou, a partir do exame do caso concreto, que, da violação a seus dados pessoais, houve a ocorrência de danos morais. Dados que não são sensíveis e são de fácil acesso a qualquer pessoa. Precedentes. Ampla divulgação da violação já realizada. Recolhimento dos dados. Inviabilidade, considerando-se a ausência de finalização das investigações. Pedidos julgados parcialmente procedentes, todavia, com o reconhecimento da ocorrência de vazamento dos dados pessoais não sensíveis da autora e condenando-se a ré na apresentação de informação das entidades públicas e privadas com as quais realizou o uso compartilhado dos dados, fornecendo declaração completa que indique sua origem, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, assim como a cópia exata de todos os dados referentes ao titular constantes em seus bancos de dados, conforme o art. 19, II, da LGPD. Determinação para envio de cópia dos autos à Autoridade Nacional de Proteção de Danos (art. 55-A da LGPD). RECURSO PARCIALMENTE PROVIDO, COM DETERMINAÇAO."* (fl. 1.011 e-STJ).

Os embargos de declaração foram rejeitados (e-STJ fls. 1.036/1.039).

No recurso especial, a recorrente alega violação dos arts. 18, VII, 19, II, 42, 43, III, e 46, *caput*, da Lei 13.709/2018 ("Lei Geral de Proteção de Dados Pessoais - LGPD"), no sentido de que a obrigação de fornecer declaração completa que indique a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, assim como a cópia exata de todos os dados referentes ao titular constantes em seus bancos de dados, referir-se-ia às hipóteses de compartilhamento lícito de dados pessoais. Entretanto, defende que o caso dos autos configura-se como compartilhamento ilícito, decorrente de ataque cibernético.

As contrarrazões não foram apresentadas (fl. 1.137 e-STJ) e o recurso foi inadmitido na origem, dando ensejo à interposição de agravo, que foi provido para determinar a subida do especial (fls. 1.167/1.168 e-STJ).

VOTO

> *O tratamento de dados pessoais, em particular por processos automatizados, é, no entanto, uma atividade de risco. Risco que se concretiza na possibilidade de exposição e utilização indevida ou abusiva de dados pessoais, na eventualidade desses dados não serem corretos e representarem erroneamente seu titular, em sua utilização por terceiros sem o conhecimento deste, somente para citar algumas hipóteses reais. Daí resulta ser necessária a instituição de mecanismos que possibilitem à pessoa deter conhecimento e controle sobre seus próprios dados – que, no fundo, são expressão direta de sua própria personalidade. Por este motivo, a proteção de dados pessoais é considerada em diversos ordenamentos jurídicos como um instrumento essencial para a proteção da pessoa humana e como um direito fundamental.*
>
> **Danilo Doneda**, "A proteção dos dados pessoais como um direito fundamental." Espaço Jurídico Journal of Law, [S.l.], v. 12, n. 2, p. 91–108, 2011.
> *Disponível em: https://periodicos.unoesc.edu.br/espacojuridico/article/view/1315.*

1. Síntese dos fatos

Na origem, trata-se de ação de obrigação de fazer c/c indenização por danos morais proposta por THAYNA NAYARA DA SILVA QUEIROZ contra ELETROPAULO METROPOLITANA ELETRICIDADE DE SÃO PAULO S.A.

A autora alegou, em síntese, que recebeu comunicado do Instituto de Proteção de Dados Pessoais - Iprodape, do qual é associada, com notícia sobre incidente de segurança com os seguintes dados pessoais de sua titularidade: nome completo, números de RG e CPF, endereço e telefone. Informou que teve indevida exposição de sua intimidade, a autorizar a condenação da empresa ré/recorrente em danos morais, com fundamento no art. 42 e seguintes da LGPD. Narrou que a empresa não teria informado em quais circunstâncias o fato ocorreu, tampouco a identidade dos terceiros que tiveram acesso a tais dados.

A sentença julgou os pedidos improcedentes; entretanto, o TJSP deu parcial provimento à apelação, afastando a indenização por danos morais e reconhecendo a ocorrência de vazamento dos dados pessoais não sensíveis da autora/recorrida. Em virtude deste vazamento, condenou a ré/recorrente a apresentar informação das entidades públicas e privadas com as quais realizou o uso compartilhado dos dados,

fornecer declaração completa com a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, assim como a cópia exata de todos os dados referentes à titular constantes em seus arquivos.

2. Delimitação da controvérsia recursal e premissas do caso

A controvérsia jurídica consiste em definir se o vazamento de dados pessoais não sensíveis do titular, decorrente de atividade ilícita, é passível de gerar ao agente de tratamento de dados as obrigações previstas no art. 19, II, da LGPD, ou se o fato de tal vazamento ter decorrido de atividade ilícita seria uma excludente de responsabilidade, prevista no art. 43, III, da LGPD (culpa exclusiva de terceiro).

Conforme visto, o acórdão se assentou nas seguintes premissas: ***(i)*** a empresa recorrente teria sido vítima de incidente de segurança cibernética (ataque *hacker*), a partir do qual ***(ii)*** foram expostos indevidamente dados pessoais não sensíveis da recorrida (nome, número de CPF, data de nascimento, idade, telefones fixo e celular e endereço de e-mail); ***(iii)*** teria havido falha na prestação de serviços por parte da empresa, o que impõe aos agentes de tratamento a adoção de medidas de segurança e, em virtude disso, ***(iv)*** a recorrente foi condenada a apresentar as informações solicitadas pela titular, nos termos do art. 19, II, da LGPD; ***(v)*** apesar de incontroverso o vazamento dos dados, não houve condenação da recorrente em danos morais, visto que não foram comprovados pela autora/recorrida.

3. PRELIMINAR: competência de uma das Turmas da Segunda Seção

Em 7/3/2023, a Segunda Turma do STJ julgou o Agravo em Recurso Especial 2.130.619/SP, relator Ministro Francisco Falcão, que tratou de temática semelhante à que agora se analisa, qual seja, uma ação indenizatória ajuizada por particular contra a concessionária de energia elétrica ENEL, ora recorrente, pleiteando indenização por danos morais decorrentes do vazamento e do acesso de seus dados pessoais por terceiros.

Assim, tendo em vista tal precedente, considera-se oportuno reafirmar a competência desta Terceira Turma para julgar o caso em análise.

De início, é necessário esclarecer que, neste recurso especial, não se está a analisar matérias relacionadas intrinsicamente ao interesse público nem a demandas típicas de direito público, o que atrairia a competência da Primeira Seção.

Aqui, a controvérsia jurídica de fundo consiste em definir a responsabilidade civil da recorrente no tratamento de dados pessoais da titular/recorrida. Verifica-se, portanto, que a relação jurídica litigiosa do processo originário (art. 9º do RI-STJ) possui natureza privada e patrimonial, e não trata da prestação do serviço de fornecimento de energia elétrica.

Nesse cenário, é possível concluir que a natureza jurídica da controvérsia não decorre de contrato administrativo, relação que pressupõe

a participação de pessoa jurídica de direito público, mas, sim, de relação privada. Esse panorama atrai a incidência do art. 9º, § 2º, III, do RI-STJ, segundo o qual cabe à Segunda Seção processar e julgar os feitos relativos à responsabilidade civil, salvo quando se tratar de responsabilidade civil do Estado, o que não é o caso.

É por esse motivo que a Segunda Seção e suas Turmas vêm apreciando recursos que versam sobre responsabilidade civil e relação jurídica entre consumidor e concessionárias de serviço público. Nesse sentido, AgInt no AREsp 1.894.385/RJ, relatora Ministra Nancy Andrighi, Terceira Turma, julgado em 14/2/2022, DJe de 16/2/2022; REsp 1.853.361/PB, relatora Ministra Nancy Andrighi, relator para acórdão Ministro Marco Buzzi, Segunda Seção, julgado em 3/12/2020, DJe de 5/4/2021; REsp 1.872.260/SP, relator Ministro Marco Aurélio Bellizze, Terceira Turma, julgado em 4/10/2022, DJe de 7/10/2022; REsp 1.936.743/SP, relator Ministro Luis Felipe Salomão, Quarta Turma, julgado em 14/6/2022, DJe de 8/9/2022; AgInt no AREsp 1.858.297/RJ, relator Ministro Paulo de Tarso Sanseverino, Terceira Turma, julgado em 6/6/2022, DJe de 9/6/2022; REsp 1.766.638/RJ, relator Ministro Ricardo Villas Bôas Cueva, Terceira Turma, julgado em 18/10/2022, DJe de 24/10/2022, e REsp 1.677.955/RJ, relator Ministro Ricardo Villas Bôas Cueva, Terceira Turma, julgado em 18/9/2018, DJe de 26/9/2018.

4. MÉRITO

De modo breve, é importante recapitular que a Emenda Constitucional nº 115/2022, ao inscrever a proteção e o tratamento de dados pessoais no rol dos direitos e garantias fundamentais da Constituição (art. 5º, LXXIX), inaugurou um novo capítulo no ordenamento jurídico brasileiro no que tange aos direitos de personalidade, à liberdade e à autodeterminação informativa. Do mesmo modo, com a finalidade de garantir esses direitos, a lei criou para os agentes de tratamento de dados pessoais uma série de deveres e procedimentos de segurança a serem observados, com vistas a garantir a higidez e o cuidado no tratamento das informações dos titulares.

Relembre-se que, antes mesmo de positivado na Constituição, o Supremo Tribunal Federal já havia analisado o tema, oportunidade em que reconheceu a autonomia do direito fundamental à proteção de dados pessoais como categoria integrante do rol dos direitos fundamentais.

Confira-se trecho do voto da relatora, Ministra Rosa Weber, nas ADIs 6387, 6388, 6389, 6390 e 6393 MC-REF/DF (DJe 12/11/2020):

> *"III – Direito fundamental à proteção de dados pessoais*
> *(...)*
> *A adequada compreensão do parâmetro de controle invocado, no entanto, perpassa o aprofundamento do inevitável debate teórico acerca da afirmação da autonomia do direito fundamental à proteção de dados pessoais como categoria dentro do rol dos direitos fundamentais, para além da mera evolução do direito ao sigilo.*

Nesse sentido, a análise do referendo da medida cautelar nesta ADI suscita a oportunidade e o dever de o Supremo Tribunal Federal aprofundar a identificação, na ordem constitucional brasileira, de um direito fundamental à proteção de dados pessoais, a fim de estabelecer de forma clara o âmbito de proteção e os limites constitucionais à intervenção estatal sobre essa garantia individual.

(...)

*Esse processo de reinvenção do direito à privacidade é analisado com esmero e profundidade em seminal monografia do Professor Danilo Doneda (**DONEDA, Danilo**. Da privacidade à proteção de dados pessoais. Renovar: Rio de Janeiro, 2006). Ao examinar as sucessões geracionais das leis de proteção de dados a partir da década de 1970, bem como o espraiamento da proteção jurídica da privacidade em tratados internacionais ao longo do século XX, o autor assevera que:*

> *'A trajetória percorrida pelo direito à privacidade reflete tanto uma mudança de perspectiva para a tutela da pessoa quanto sua adequação às novas tecnologias da informação. Não basta pensar a privacidade nos moldes de um direito subjetivo, a ser tutelado conforme as conveniências individuais, nem da privacidade como uma 'predileção' individual, associada basicamente ao conforto e comodidade. (...)*
>
> *Uma esfera privada, na qual a pessoa tenha condições de desenvolvimento da própria personalidade, livre de ingerências externas, ganha hoje ainda mais em importância: passa a ser um pressuposto para que ela não seja submetida a formas de controle social que, em última análise, anulariam sua individualidade, cerceariam sua autonomia privada e, em última análise, inviabilizariam o livre desenvolvimento da sua personalidade.*
>
> *A privacidade assume, portanto, posição de destaque na proteção da pessoa humana, não somente tomada como escudo contra o exterior – na lógica da exclusão – mas como elemento positivo, indutor da cidadania, da própria atividade política em sentido amplo e dos direitos de liberdade de uma forma geral. Neste papel, a vemos como pressuposto de uma sociedade democrática moderna, da qual o dissenso e o anticonformismo são componentes orgânicos' (grifos nossos) (**DONEDA**, op. cit., pp. 141-142).'*

*Essa nova abordagem também engloba uma proteção abrangente que desloca o eixo da proteção do conteúdo dos dados para as possibilidades e finalidades do seu processamento. Como bem destacado pela professora Laura Schertel Mendes, é decisivo para a concepção do direito à autodeterminação 'o princípio segundo o qual não mais existiriam dados insignificantes nas circunstâncias modernas do processamento automatizado dos danos', de modo que 'o risco do processamento de dados residiria mais na finalidade do processamento e nas possibilidades de processamento do que no tipo dos dados mesmos (ou no fato que quão sensíveis ou íntimos eles são)' (**MENDES, Laura Schertel.** Autodeterminação informativa: a história de um conceito. No Prelo).*

Essa abrangência da proteção atribuída ao direito de autodeterminação constitui importante chave interpretativa do âmbito de proteção do direito fundamental à proteção de dados pessoais, o qual não recai propriamente sobre a dimensão privada ou não do dado, mas sim sobre os riscos atribuídos ao seu processamento por terceiros.

(...)

É que (...) a tutela de um direito fundamental à proteção de dados não mais se adstringe à demarcação de um espaço privado, mas, antes, afirma-se no direito à governança, transparência e sindicabilidade do tratamento de dados compreendidos em acepção abrangente".

Se antes as formas de responsabilidade civil nas questões afetas aos dados pessoais estavam circunscritas às leis civis e ao Código de Defesa do Consumidor, o microssistema introduzido pela LGPD criou, ampliou e consolidou balizas para tratar do assunto, sob o prisma da proteção aos direitos fundamentais.

Aliás, a doutrina tem debatido quanto à natureza da responsabilidade civil prevista pela LGDP. Para além da clássica dicotomia entre as vertentes objetiva e subjetiva, há autores que defendem um novo sistema de responsabilização, denominado de responsabilidade civil proativa, conforme consignado pelo TJSP.

Nessa leitura, *"[a] nova lei, porém, introduz, secundando o regulamento europeu, uma mudança profunda em termos de responsabilização. Trata-se da sua união ao conceito de 'prestação de contas'. Esse novo sistema de responsabilidade, que vem sendo chamado de 'responsabilidade ativa' ou 'responsabilidade proativa' encontra-se indicada no inciso X do art. 6º, que determina que às empresas que não é suficiente cumprir os artigos da lei; será necessário também 'demonstrar a adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, a eficácia dessas medidas. Portanto, 'não descumprir a lei, não é mais suficiente'. (...) Exige-se, em síntese, atitudes conscientes, diligentes e proativas por parte das empresas em relação à utilização dos dados pessoais. Assim, a partir de agosto de 2020, quando entra em vigor a LGPD, qualquer empresa que processe dados pessoais, terá não apenas que cumprir a lei, mas também terá que provar que está em conformidade com a Lei. Caberá às empresas, em vez de à Administração Pública, a responsabilidade de identificar os próprios riscos e escolher e aplicar as medidas apropriadas para mitigá-los."* (Maria Celina Bodin de Moraes e João Quinelato de Queiroz, "Autodeterminação informativa e responsabilização proativa", Cadernos Adenauer XX (2019) nº 3, p. 113).

No que interessa ao presente caso, registra-se que referida lei estabeleceu diversas definições relacionadas aos bens jurídicos protegidos, tais como ***(i)*** dado pessoal, que é a informação relacionada à pessoa natural identificada ou identificável; ***(ii)*** titular, a pessoa natural a quem se referem os dados pessoais que são objeto de tratamento; ***(iii)*** controlador, identificado pela pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais; ***(iv)*** operador, que é pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador, e ***(v)*** agentes de tratamento, definidos pelo controlador e pelo operador.

A norma também definiu o papel dos atores envolvidos no ecossistema da proteção de dados (art. 5º), os direitos do titular (arts. 17 a 22), os requisitos para o tratamento dos dados pessoais e a forma de responsabilidade e de ressarcimento de danos (arts. 42 a 45). Some-se a isso o decálogo de princípios que devem ser observados nas atividades de tratamento de dados: finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção,

não discriminação e responsabilização e prestação de contas, somados à boa-fé (art. 6º LGPD).

Dentre tais princípios, a hipótese ora analisada dá relevo à transparência, fundada na garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial; à segurança, referente à utilização de medidas 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 difusão; à prevenção, ao adotar medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais, e responsabilização e prestação de contas, relativos à demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Dadas todas essas definições, ao se verificar que a empresa recorrente se enquadra na categoria dos agentes de tratamento, caberia a ela tomar todas as medidas de segurança esperadas pelo titular para que suas informações fossem protegidas, entre as quais a utilização das técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado. Em acréscimo, os sistemas utilizados para o tratamento de dados pessoais da recorrente deveriam estar estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos na LGPD e às demais normas regulamentares (art. 49).

Além do mais, a legislação sugere uma série de procedimentos, de ferramentas e de condutas a serem atendidas pelos agentes de tratamento com a finalidade de evitar incidentes de segurança, como, por exemplo, formular regras de governança, normas de segurança e mecanismos internos de supervisão e de mitigação de riscos relacionados ao tratamento de dados pessoais (art. 50).

Todo esse esforço de conformidade e de aplicação da LGPD nas atividades das empresas que lidam com tratamento de dados, e também do poder público, é conhecido como *compliance* de dados. A transparência, o fiel cumprimento das normas e o dever de prestar contas passam a ser promovidos por instrumentos que induzem não apenas à obediência ao direito, mas também à comprovação da efetividade dos programas de conformidade.

Nesse quadro, é fácil perceber que os programas de *compliance* de dados, com ênfase na transparência e no dever de prestar contas (*accountability*), são destinados a transformar de modo duradouro a própria ideia matriz dos programas de cumprimento de normas.

No que se refere ao alegado incidente de segurança (ataque *hacker*), é de se registrar que ataques cibernéticos destinados a identificar vulnerabilidades de segurança em diversos sistemas e a obter o maior número possível de dados tornam-se cada vez mais frequentes. Os incidentes de *data breaches* ou vazamentos de dados consistem em situações nas quais um grande volume de informações pessoais (tais

como nome, endereço, números de documentos, dados bancários, credenciais de acesso, entre outros) é extraído, resultando em consequências aos seus titulares, dependendo da extensão do ataque. No longo prazo, a falta de elementos capazes de garantir a segurança da informação podem levar a uma verdadeira corrosão da privacidade, na qual dados sensíveis relacionados à identidade dos indivíduos podem ser indevidamente apropriados por terceiros de maneira contínua e indeterminada.

Entretanto, um vazamento de dados nem sempre será reconhecido como fortuito externo, portanto apto a elidir a responsabilidade civil do agente. A doutrina assevera que *"poder-se-ia definir a ação como fortuito interno, uma vez que a segurança de um sistema informático que lide com informações sensíveis é um pressuposto a ser esperado da atividade empresarial. Exemplificadamente, a adoção de padrões mínimos de autenticação e autorização de acesso a aplicações na rede, como o protocolo HTTPS, é pressuposto para o funcionamento e a confiança em serviços na internet. Comparativamente, a Súmula nº 479 do Superior Tribunal de Justiça estipula que delitos praticados por terceiros no âmbito de operações bancárias configuram-se fortuito interno da atividade, desencadeando responsabilização objetiva das instituições financeiras."* (Jordan Vinícius de Oliveira. Revista Brasileira de Direito Civil – RBDCivil, v. 31, n. 1, p. 17-56, jan./mar. 2022).

Da mesma forma, o tratamento de dados pessoais ora analisado 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 (art. 44, III, da LGPD).

Assim, ao não provar, perante as instâncias de origem, que o vazamento dos dados da recorrida teria se dado exclusivamente em razão do incidente de segurança, é impossível aplicar em favor da recorrente a excludente de responsabilidade do art. 43, III, da LGPD. No artigo mencionado, a técnica de redação legislativa deixa claro que os agentes de tratamento *"só não serão responsabilizados quando **provarem** que o dano é decorrente de **culpa exclusiva** do titular dos dados ou **de terceiro**"* (destacou-se), deixando claro o ônus legal deste ente em provar a quebra do nexo causal nessas hipóteses.

No que tange à distribuição do ônus probatório, é relevante destacar que o art. 42, § 2º, da lei de regência prevê a possibilidade de inversão do ônus da prova, a critério do magistrado, em benefício do titular dos dados, desde que a alegação seja admissível, que haja hipossuficiência do titular para a produção da prova ou que a sua produção, pelo titular, se mostre por demais onerosa. Disposições acerca da redistribuição ou da inversão do ônus da prova também se encontram em outras legislações, como no art. 373, § 1º, do Código de Processo Civil, bem como no art. 6º, inciso VIII, do CDC.

Diante desse cenário, o agente de tratamento responderá pelas violações da segurança dos dados. Também incorrerá em responsabilidade por deixar de

adotar medidas de segurança técnicas e administrativas aptas a proteger os dados pessoais da recorrida de acessos não autorizados (incidentes de segurança e ataques *hacker*), e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito (art. 46 da LGPD).

Daí porque está correta a conclusão do TJSP ao aplicar os direitos do titular e condenar a recorrente na obrigação de apresentar informação das entidades públicas e privadas com as quais realizou o uso compartilhado dos dados da recorrida (art. 18, VII, da LGPD) e a fornecer declaração completa que indique a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, assim como a cópia exata de todos os dados referentes ao titular constantes em seus bancos de dados (art. 19, II, da LGPD).

Em suma, as teses veiculadas pela recorrente não merecem acolhida, pois, ainda que o vazamento tivesse decorrido exclusivamente de um incidente ilícito de segurança, não há elementos mínimos no acórdão impugnado de que a empresa tivesse lançado mão das medidas de segurança estabelecidas pela LGPD, que pudessem ser necessárias e suficientes à proteção dos dados pessoais da recorrida. Além do mais, também não há como imputar culpa exclusiva de terceiro no evento, ante a inexistência de provas de tal fato.

5. Conclusão

Ante o exposto, conheço do recurso especial e nego-lhe provimento.

Nos termos do art. 85, § 11, do CPC, os honorários sucumbenciais devem ser majorados para R$ 10.000,00 (dez mil reais), atualizados desde o arbitramento na origem.

É o voto.

CERTIDÃO DE JULGAMENTO
TERCEIRA TURMA

Número Registro: 2022/0220922-8 **PROCESSO ELETRÔNICO** **REsp 2.147.374 / SP**

Números Origem: 10007945920218260554 10007945920218260554500000 20210000978294

PAUTA: 03/12/2024 JULGADO: 03/12/2024

Relator
Exmo. Sr. Ministro **RICARDO VILLAS BÔAS CUEVA**

Presidente da Sessão
Exmo. Sr. Ministro HUMBERTO MARTINS

Subprocurador-Geral da República
Exmo. Sr. Dr. ONOFRE DE FARIA MARTINS

Secretária
Bela. MARIA AUXILIADORA RAMALHO DA ROCHA

AUTUAÇÃO

RECORRENTE	:	ELETROPAULO METROPOLITANA ELETRICIDADE DE SAO PAULO S.A.
ADVOGADO	:	GUSTAVO ANTONIO FERES PAIXAO - SP186458A
RECORRIDO	:	THAYNA NAYARA DA SILVA QUEIROZ
ADVOGADO	:	ADILSON ALMEIDA DE VASCONCELOS - SP146989
INTERES.	:	ENEL DISTRIBUIÇÃO SAO PAULO S/A
ADVOGADO	:	GUSTAVO ANTONIO FERES PAIXAO - SP186458

ASSUNTO: DIREITO CIVIL - Lei Geral de Proteção de Dados (LGPD) - Proteção de Dados Pessoais

CERTIDÃO

Certifico que a egrégia TERCEIRA TURMA, ao apreciar o processo em epígrafe na sessão realizada nesta data, proferiu a seguinte decisão:

A TERCEIRA TURMA, por unanimidade, negou provimento ao recurso especial, nos termos do voto do Sr. Ministro Relator.

Os Srs. Ministros Nancy Andrighi, Humberto Martins e Moura Ribeiro votaram com o Sr. Ministro Relator.Presidiu o julgamento o Sr. Ministro Humberto Martins.