

Relatório Painel LGPD nos Tribunais 2026

Relatório Painel LGPD nos Tribunais

3ª Edição

São Paulo

2026

COPYRIGHT©2026
CEDIS-IDP e Jusbrasil

PRODUÇÃO EDITORIAL
CEDIS-IDP

REVISÃO
CEDIS-IDP

PROJETO GRÁFICO E DIAGRAMAÇÃO
Equipe Jusbrasil

Todos os direitos reservados ao Cedis-IDP e ao Jusbrasil. É vetada a reprodução por qualquer meio mecânico, eletrônico, xerográfico etc., de parte ou totalidade do material sem a permissão por escrito da detentora dos direitos.

Equipe Painel LGPD

Diretores do CEDIS-IDP

Laura Schertel Mendes
Victor Fernandes

Idealizadores do Projeto

Laura Schertel Mendes
Danilo Doneda
Bráulio Gusmão

Coordenação Científica do Painel LGPD nos Tribunais

Laura Schertel Mendes
Mônica Fujimoto

Coordenadoras do Painel LGPD no Cedis/IDP

Eduarda Costa
Mônica Fujimoto
Sayuri Pacheco Hamaoka

Organização e Revisão do Relatório

Eduarda Costa
Laura Schertel Mendes
Mônica Fujimoto
Sayuri Pacheco Hamaoka

Redação do Relatório

Camila Cristina da Silva
Eduarda Costa
Giovanna Milanese
Mônica Fujimoto
Paula Pedigoni Ponce
Sayuri Pacheco Hamaoka

Equipe Jusbrasil

Anna Catarina Alves
Marcella Ferreira
Pedro Colombini
Victor Jacó
Lara Canda
Gustavo Maia
Luiz Paulo Pinho
Rafael Costa

Pesquisadores voluntários no Cedis/IDP

Ana Elvira Alves
Bruna Luíza Motta Adorno
Bruna Presmic
Cacyone Gomes Barbosa Gonçalves Lavareda
Camila Cristina da Silva
Daniela Nunes dos Santos Ferreira
Gabriele Camillo Seitenfus
Giovanna Diniz Eduardo
Izabelly Karoline Romão Santos
Larissa Bárbara dos Santos Lourenço
Luiza Rafaela Vasconcelos Chaffim
Manuela de Oliveira Souza Brito
Milena de Bonis Faria
Rodrigo de Carvalho Assumpção
Rodrigo Toledo Costa de Almeida
Samira Borelli Satriano
Thálisson de Oliveira Lopes
William Coser Stoffels
Yasmim Beatriz Silveira Santos

Apresentação da Quinta Edição do Painel

pelas Coordenadoras do Projeto

O Painel LGPD nos Tribunais é uma iniciativa do Centro de Direito, Internet e Sociedade (Cedis/IDP) em parceria com o Jusbrasil e apoio do Programa das Nações Unidas para o Desenvolvimento (PNUD Brasil). O projeto se dedica a estudos avançados sobre proteção de dados e direitos fundamentais no Brasil, e ao mapeamento de possíveis tendências e posicionamentos nos Tribunais no desenvolvimento de uma cultura de proteção de dados no Brasil desde a entrada em vigor da Lei Geral de Proteção de Dados (LGPD – Lei no 13.709/2018) em setembro de 2020.

Assim, essa edição especial marca a celebração dos 5 anos de trajetória deste projeto, idealizado e dirigido por dois dos maiores especialistas do tema no país, Danilo Doneda (in memoriam) e Laura Schertel Mendes, juntamente com o juiz do trabalho Braulio Gusmão. A iniciativa conta com a coordenação científica da Diretora do Cedis/IDP Laura Schertel, ao lado da professora Mônica Fujimoto. A coordenação responsável pelo desenvolvimento deste projeto no Cedis/IDP foi composta pela professora Mônica Fujimoto e pelas pesquisadoras Sayuri Pacheco Hamaoka e Eduarda Costa Almeida.

Além disso, neste ano foi selecionado um número reduzido de pesquisadores para que a parte técnica fosse mais robusta e a análise das decisões mais profunda. Assim, a análise das decisões contou com a participação de 18 pesquisadores voluntários e de membros do Cedis/IDP, aos quais agradecemos profundamente pela sua dedicação. Além dos membros regulares do Cedis/IDP e dos pesquisadores voluntários, a pesquisa conta com a essencial participação dos

colaboradores do Jusbrasil no desenvolvimento de busca dos julgados em todas as edições. A equipe técnica envolve-se em todas as etapas da pesquisa, desde a extração dos dados até o desenvolvimento de ajustes necessários ao longo do processo de análise. O Jusbrasil concede acesso aos pesquisadores, em sua plataforma, à íntegra das decisões a serem analisadas, que são selecionadas por meio de algoritmos desenvolvidos por sua equipe. Os dados levantados pelo Jusbrasil são de acesso público e foram coletados junto a diferentes diários oficiais eletrônicos e nas páginas de pesquisa de jurisprudência do Poder Judiciário.

O trabalho executado pelo Jusbrasil ficou a cargo de Anna Catarina Alves, Cecília Veloso, Heloisa Bianchini, Marcella Ferreira, Pedro Colombini e Víctor Jacó.

Ao longo dos 5 anos de existência do projeto buscamos colaborar com o debate brasileiro dedicado à matéria de proteção de dados pessoais a partir de julgados no âmbito do Poder Judiciário, oferecendo à comunidade jurídica e científica um panorama atualizado e, até então, inédito dos casos julgados sobre o tema. As decisões podem ser buscadas na íntegra por meio do sítio eletrônico do Painel LGPD nos Tribunais, que conta com um buscador e filtros de busca de jurisprudência especialmente dedicados à proteção de dados pessoais.

Ao longo de suas cinco edições, o Painel LGPD nos Tribunais consolidou-se como um instrumento empírico de acompanhamento da incorporação da proteção de dados pessoais pelo Poder Judiciário brasileiro, permitindo não apenas o mapeamento quantitativo das decisões, mas, principalmente, a identificação de padrões de interpretação, tensões normativas e trajetórias de amadurecimento jurisprudencial.

Primeira edição (out/2020 – out/2021)

No primeiro ciclo da pesquisa, iniciado assim que a LGPD entrou em vigor, o esforço esteve concentrado na identificação inicial de decisões relevantes, tendo sido analisados 274 julgados, com o apoio de aproximadamente 50 pesquisadores. Tratava-se, à época, de um cenário ainda marcado por referências incipientes à Lei, frequentemente de caráter principiológico e com baixa densidade argumentativa, ou mesmo de citações à lei desacompanhadas de menções expressas aos seus artigos.

Nesse primeiro ciclo, acontecimentos relevantes marcaram os debates sobre tecnologia, como foi o caso do julgamento do RE 1.010.606 (Tema 786), em que o Supremo Tribunal Federal enfrentou diretamente a ideia de “direito ao esquecimento” no ordenamento brasileiro, compreendido como a possibilidade de impedir a divulgação lícita de fatos verídicos. A Corte reconheceu, contudo, que situações concretas devem ser analisadas à luz de outros direitos constitucionais, como honra, imagem e privacidade.

No mesmo período, entraram em vigor as sanções administrativas da LGPD, sendo acompanhada pela edição da Resolução CD/ANPD no 1/2021, que instituiu o Regulamento de Fiscalização e do Processo Administrativo Sancionador. A norma estabeleceu a estrutura procedimental da atuação sancionatória da ANPD, definindo etapas, competências e mecanismos de apuração, decisão e recurso, e conferindo maior previsibilidade ao enforcement da legislação na seara administrativa.

Segunda edição (out/2021 – out/2022)

A partir da segunda edição, a LGPD passou a ser citada como fundamento decisório de forma mais robusta, sendo identificado, inclusive, o surgimento de divergências interpretativas quanto à sua aplicação. Destaca-se, nesse contexto, a controvérsia relativa à caracterização do dano moral *in re ipsa* em casos de incidentes de segurança envolvendo dados pessoais. Nas hipóteses em que titulares pleitearam indenização por vazamento ou uso indevido de dados, a jurisprudência mostrou-se dividida sendo identificado de um lado, decisões que reconhecem a presunção do dano moral; de outro, julgados que exigem a demonstração concreta de prejuízo para sua configuração .

Também nesse ano foi aprovada a Emenda Constitucional no 115 de 2022, consagrando a positivação do direito fundamental à proteção de dados. A alteração constitucional assegura a tutela de dados em meios físicos e digitais e atribui à União competência privativa para legislar sobre a matéria, bem como para organizar e fiscalizar sua proteção, reforçando o papel institucional da ANPD, que nesse ano também foi transformada em autarquia especial por meio da promulgação da Lei no 14.460/2022.

Outro marco relevante desse período foi o julgamento da ADI 6649 e da ADPF 695 pelo STF, no qual se reconheceu a possibilidade de compartilhamento de dados pessoais entre órgãos da Administração Pública federal. A Corte, contudo, condicionou essa prática à observância de salvaguardas, como a limitação ao mínimo necessário para a finalidade pretendida, o registro de acessos e a adoção das garantias previstas na LGPD.

Terceira edição (out/2022 – out/2023)

Na terceira edição, o projeto registrou um crescimento expressivo no volume de decisões analisadas, marcando um volume 400% superior em relação à edição anterior. Esse maior volume também foi acompanhado por uma maior diversidade temática nos casos apreciados pelos tribunais. Nesse contexto, foi necessária uma mudança na apresentação do resultado da pesquisa, buscando-se maior aprofundamento analítico e sendo este o primeiro ano de publicação do Relatório Painel LGPD nos Tribunais.

Nesta edição consolidaram-se debates que continuaram centrais nos anos seguintes, como o uso de dados pessoais no ambiente de trabalho, especialmente em práticas de monitoramento e geolocalização, e a responsabilização por incidentes de segurança. A pesquisa também evidenciou um desafio metodológico relevante, qual seja a elevada incidência de decisões que apenas mencionavam a LGPD sem incorporá-la de forma efetiva à *ratio decidendi*, o que demandou o refinamento dos critérios de seleção e relevância.

O tema da geolocalização ganha destaque particular nesse período. Sua crescente utilização no contencioso trabalhista como ferramenta de controle de jornada, comprovação de atividade e monitoramento de trabalhadores em deslocamento evidenciou a tensão entre o exercício regular de direitos, nos termos do art. 7º, VI, da LGPD, e os princípios de finalidade, necessidade e proporcionalidade. Ao mesmo tempo, a expansão das plataformas de trabalho sob demanda ampliou o debate sobre a aplicação do art. 20 na revisão de decisões automatizadas. Dados coletados por aplicativos de transporte e entrega, como localização em tempo real, histórico de rotas e sistemas de avaliação automatizada, passaram a ser questionados quanto à base legal que legitima seu tratamento e ao uso dessas informações em decisões que impactam diretamente a renda e o acesso dos trabalhadores às plataformas.

Nos tribunais superiores dois julgados se destacam. O primeiro é o julgamento da ADC 51 pelo Supremo Tribunal Federal, que reafirmou a possibilidade de requisição direta de dados a provedores estrangeiros com sede ou representantes no Brasil, demonstrando a complexidade dos debates sobre a extraterritorialidade das plataformas digitais e a importância da garantia da soberania jurisdicional brasileira sobre plataformas que atuam no país. O segundo é o julgamento do AREsp 2.130.619/SP pelo STJ, em março de 2023, no qual se firmou o entendimento de que o vazamento de dados pessoais não sensíveis não gera,

por si só, dano moral presumido, sendo necessária a comprovação de prejuízo concreto. Esse precedente tornou-se referência no debate sobre responsabilidade civil e marcou o início de uma tensão interpretativa que se aprofundaria nas edições subsequentes. Adicionalmente, merece destaque a aplicação, nesse período, da primeira sanção administrativa pela ANPD por descumprimento da LGPD no âmbito do Processo Administrativo Sancionador no 00261.000489/2022-62 envolvendo a empresa Telekall. No caso concreto, verificou-se a oferta de listas de contatos de WhatsApp para fins de disseminação de propaganda eleitoral, evidenciando o uso indevido de dados pessoais. Nesse contexto, a ANPD consignou que a empresa deixou de cumprir obrigações legais previstas na legislação, além de não indicar encarregado pelo tratamento de dados pessoais.

Quarta edição (out/2023 – out/2024)

Na quarta edição, o projeto atingiu maior maturidade metodológica e passou a refletir, com mais precisão, o próprio amadurecimento da jurisprudência. Sob a perspectiva metodológica da avaliação das decisões no painel, introduziu-se a exigência de menção expressa a dispositivos específicos da LGPD como critério de relevância. Essa decisão foi motivada pela mudança qualitativa das decisões analisadas, uma vez que a lei deixou de ser majoritariamente invocada como referência genérica para ser aplicada como fundamento decisório mais profundo, com indicação de artigos, princípios e hipóteses de tratamento específicas.

Dois temas ganham centralidade no contencioso desse período. O primeiro é a articulação entre a LGPD e o Código de Defesa do Consumidor em casos de fraude bancária e incidentes de segurança. O julgamento do REsp 2.077.278/SP pela Terceira Turma do STJ introduziu a lógica da responsabilidade objetiva nesse contexto. No caso, a Ministra Relatora Nancy Andrighi reconheceu a responsabilidade da instituição financeira por vazamento de dados que viabilizou fraude contra o titular, reforçando a convergência entre os dois regimes normativos como instrumento de tutela do consumidor digital.

O segundo tema foi a aplicação da LGPD em decisões automatizadas envolvendo perfis de motoristas de aplicativos, no âmbito do REsp 2.135.783. No julgamento, o STJ reconheceu que as informações utilizadas para o descredenciamento do motorista configuram dados pessoais, atraindo a incidência da LGPD, e afirmou que decisões automatizadas que impactam o perfil profissional do titular devem observar os princípios da transparência e do direito à revisão (art. 20). Nesse sentido, entendeu-se que, embora não seja necessária a notificação prévia para a suspensão do perfil em situações que envolvam riscos à plataforma ou aos usuários, deve ser assegurado ao motorista o acesso às razões da decisão e a possibilidade de exercício do contraditório e da ampla defesa em momento posterior, inclusive com a possibilidade de revisão da decisão adotada.

A quinta edição (out/2024 – out/2025) em perspectiva: amadurecimento jurisprudencial e agenda futura

A quinta edição se insere em um momento de consolidação e transição. Com mais de 24 mil decisões coletadas e 5.555 analisadas em profundidade, esta edição do painel evidencia a consolidação da LGPD como elemento estruturante do contencioso brasileiro. Com a evolução jurisprudencial naturalmente também surgem novos desafios e fica ainda mais importante a compreensão sobre os diferentes modos pelos quais a legislação é interpretada, tensionada e integrada a outros regimes jurídicos, como o CDC, o direito do trabalho e, crescentemente, o direito constitucional digital.

Nesta edição uma decisão importante marcou o debate sobre responsabilidade civil por incidentes de segurança, que nos anos anteriores havia oscilado entre a exigência de dano concreto e a presunção de dano moral para dados sensíveis. O REsp 2.147.374-SP, julgado em dezembro de 2024 pelo ministro Ricardo Villas Bôas Cueva e publicado no Informativo 838, abordou especificamente a questão da imputação da responsabilidade civil em casos de ataque cibernético externo. O acórdão consolidou uma lógica de responsabilização baseada em accountability: o agente de tratamento não pode se eximir de responsabilidade simplesmente alegando que o incidente foi causado por terceiros, sendo-lhe imposta a demonstração de que adotou medidas efetivas de segurança ou, alternativamente, a prova de que o ataque externo foi causa exclusiva do dano. Trata-se de entendimento que avança sobre a estrutura causal da responsabilidade civil.

Além desse tema, outro debate retoma o posicionamento apresentado no âmbito do AREsp 2.130.619/SP, julgado em 2023 pela Segunda Turma com Relatoria do Ministro Francisco Falcão, que permanece como referência para a exigência de demonstração de prejuízo concreto nos casos envolvendo dados pessoais não sensíveis.

Trata-se do entendimento apresentado no âmbito do REsp 2.201.694/SP, julgado em agosto de 2025 pela Terceira Turma, sob a relatoria da ministra Nancy Andrighi, reconheceu a possibilidade de dano moral presumido mesmo em casos envolvendo dados pessoais não sensíveis. Com fundamento na violação à autodeterminação informativa como bem jurídico autônomo tutelado pela LGPD e pela Emenda Constitucional no 115/2022, o acórdão afastou a

exigência de prova de prejuízo efetivo, entendendo que a própria disponibilização indevida de dados, ainda que cadastrais ordinários, é suficiente para configurar dano in re ipsa. A decisão coloca em tensão direta o entendimento reafirmado no AREsp 2.130.619/SP e sinaliza uma inflexão interpretativa relevante dentro da própria Terceira Turma.

O cenário se torna ainda mais complexo ao se considerar que, em novembro de 2025, a Quarta Turma, no REsp 2.221.650/SP, sob relatoria da ministra Isabel Gallotti, adotou posição distinta, exigindo a demonstração de efetiva lesão ou prejuízo concreto. Essa divergência, ainda não pacificada, configura um dos principais pontos de atenção para o próximo ciclo.

Outro tema que deve ganhar centralidade é a afetação dos Recursos Especiais no 2.226.946/SP e no 2.226.097/SP, em dezembro de 2025. Embora não integrem o recorte amostral desta edição, que se encerra em outubro de 2025, tais recursos tratam da licitude da disponibilização ou comercialização de dados pessoais não sensíveis por gestores de bancos de dados de proteção ao crédito, sem prévia comunicação ou consentimento do titular.

Trata-se de tema que vem sendo acompanhado pelos pesquisadores do painel desde a primeira edição e que certamente é central no âmbito dos debates sobre proteção de dados no judiciário, figurando entre os principais temas objeto de manifestação do judiciário ao longo das cinco edições.

Outro tema que também vem sendo destacado desde a primeira edição e que ao longo dos últimos 5 anos é o exercício do direito dos titulares de revisão às decisões automatizadas previsto no art. 20 da LGPD. Mesmo com o posicionamento do STJ sobre o tema no âmbito do REsp 2.135.783 as decisões ainda oscilam quanto às conclusões dos casos, pois parte delas reconhece a impossibilidade de bloqueio sem defesa ou revisão humana, aplicando danos morais, bem como a reativação da conta, enquanto outras consideram que mesmo com o bloqueio da conta de forma automatizada, é necessário que se comprove o pedido de revisão para eventual aplicação de dano moral.

Por fim, destacam-se dois marcos normativos que encerraram o ano de 2025 e que certamente vão influenciar a agenda regulatória e jurisprudencial para os próximos anos. Foi aprovada a Lei no 15.211/2025, o ECA Digital, que expandiu substancialmente as obrigações de proteção de dados de menores, criando requisitos de verificação de idade para plataformas digitais e restringindo as bases legais aplicáveis ao tratamento de dados de crianças e adoles-

centes. Trata-se de tema pouco explorado nos últimos 5 anos pelo judiciário brasileiro sob a perspectiva da LGPD e que espera-se que seja objeto de debate nos próximos anos.

Reforçamos que este Relatório tem por objetivo identificar e sistematizar as principais controvérsias judiciais relacionadas à LGPD, oferecendo, por meio de pesquisa empírica, um panorama atualizado anualmente. Com isso, busca-se fomentar o debate qualificado sobre o tema, ampliar a conscientização social, contribuir para o aprimoramento de teses jurídicas e pesquisas acadêmicas, e reforçar a importância do diálogo institucional entre academia, Poder Judiciário, mercado e órgãos públicos, em especial a Autoridade Nacional de Proteção de Dados.

É com imensa alegria que desejamos a todos e todas uma ótima leitura da quinta edição do Painel LGPD nos Tribunais!

Laura Schertel Mendes
Mônica Fujimoto

Relatório do Painel LGPD nos Tribunais

Sumário

1. Notas Metodológicas	16
2. Raio-X do Painel LGPD 2025	26
2.1. Panorama Geral dos Processos Analisados	28
3. Destaques Sobre Decisões Relevantes	34
3.1. Menção a artigos da LGPD	36
3.2. Principais Setores Envolvidos	51
3.3. Ramos do Direito Correlatos à Proteção de Dados Pessoais	54
4. Questões Essenciais Sobre a Aplicação da LGPD pelos Tribunais	72
4.1. Princípios	74
4.2. Bases Legais	93
4.3. Exercício de Direitos do Titular	110
4.4. Responsabilidade	124
4.5. Incidentes de Segurança	149
5. Considerações Finais	172

PAINEL LGPD NOS TRIBUNAIS

1

Notas Metodológicas

O Painel LGPD nos Tribunais tem como objetivo central a compreensão de como os tribunais brasileiros aplicam e interpretam o tema de proteção de dados pessoais em suas decisões. A pesquisa busca respostas para questionamentos tais como: "De que forma a LGPD vem sendo interpretada pelos tribunais?"; "Quais as principais discussões sobre proteção de dados pessoais identificadas no mérito das decisões judiciais?"; "Qual o nível de profundidade das discussões?"; "Como o tema de proteção de dados pessoais dialoga com outras disciplinas do Direito?"; "Quais setores que mais demandam ou são demandados a respeito da temática?" e "Quais 'penalidades' ou 'determinações' estão sendo aplicadas pelo Poder Judiciário com fundamento na proteção de dados pessoais?".

A pesquisa tem por escopo a análise de decisões que alcancem os seguintes 3 critérios, que foram verificados: i) decisões que sejam de alta relevância; ii) decisões que contenham menções expressas a dispositivos da LGPD; e iii) decisões que sejam sentenças ou acórdãos.

A escolha desta nova segmentação deve-se à necessidade de selecionar decisões mais relevantes para compreender como o tema da proteção de dados pessoais vem sendo adotado nos tribunais - embora outras decisões tão relevantes quanto possam ser suprimidas, involuntariamente, do espaço amostral final selecionado. Diante disso, destaca-se que a pesquisa não pretende esgotar a avaliação das decisões proferidas pelo Poder Judiciário, mas sim compreender padrões de interpretação e uso da LGPD, sob uma perspectiva macro, mas igualmente ressaltar, sob um olhar minucioso, nuances de decisões interessantes.

O critério de classificação final dos níveis de relevância, após sucessivos ajustes metodológicos, foi estruturado da seguinte forma: nível 1, para decisões em que a referência à LGPD ou à proteção de dados tem caráter instrumental, burocrático ou meramente citacional; nível 2, para casos em que há apenas menção ao tema da proteção de dados, sem efetivo aprofundamento jurídico;

nível 3, para hipóteses em que há debate incidental sobre a LGPD, com fundamentação consistente em matéria de proteção de dados, ainda que a legislação não seja determinante para o desfecho da controvérsia; e nível 4, para decisões em que a LGPD constitui a questão central do caso.

Para otimizar a uniformidade da formação do espaço amostral e da classificação das decisões, foram incorporadas à ferramenta de IA do Jusbrasil instruções mais detalhadas sobre cada nível de relevância, com delimitações conceituais específicas e exemplos ilustrativos. Esse processo foi acompanhado de refinamento humano contínuo ao longo de todas as etapas da pesquisa, de modo a calibrar os critérios adotados e reduzir assimetrias classificatórias. O aperfeiçoamento dessa metodologia buscou padronizar, da forma mais consistente possível, a seleção das decisões efetivamente relevantes. Esse esforço tornou-se especialmente necessário diante do amadurecimento progressivo da jurisprudência sobre a LGPD nos tribunais brasileiros e do aumento expressivo de decisões que passaram a mencionar a legislação, nem sempre de maneira juridicamente substantiva.

Assim, na 5ª edição, ampliou-se o uso dos modelos de IA do Jusbrasil, com maior automação do processo e incorporação de informações que, nas edições anteriores, eram preenchidas manualmente pelos pesquisadores. Essa evolução buscou aumentar a escalabilidade da pesquisa, sem afastar as etapas sucessivas de refinamento metodológico e de conferência humana.

Para viabilizar a seleção das decisões e a extração das informações relevantes de cada caso, foi necessário desenvolver comandos capazes de orientar de forma reproduzível a atuação dos modelos de IA. A sistematização de critérios qualitativos e a definição da amostra dentro de um universo amplo de decisões exigiram, por isso, revisões periódicas, voltadas ao aperfeiçoamento desses parâmetros, ao seu alinhamento com os objetivos da pesquisa e à verificação de como tais instruções eram efetivamente compreendidas e operacionalizadas pelos modelos. Como será observado, a delimitação das decisões adstritas ao escopo da pesquisa é realizada pelo Cedis/IDP e implementada pelo Jusbrasil.

Os tipos de informações, bem como os conteúdos a serem extraídos, foram delimitados pelo Cedis/IDP. O grupo, com o apoio de pesquisadores voluntários e em articulação com o Jusbrasil, definiu os dados a serem extraídos de cada uma das decisões que compõem o espaço amostral da pesquisa. A partir da fixação desses parâmetros, o Jusbrasil foi responsável por operacionalizar esses critérios de acordo com sua parametrização em linguagem e coman-

dos técnicos em seus sistemas de IA.

Nesta quinta edição, o marco temporal adotado é o período de publicação de decisões entre 2 de outubro de 2024 e 1º de outubro de 2025. As datas da coleta referem-se ao dia em que as decisões foram publicadas no diário oficial eletrônico e nas páginas de pesquisa de jurisprudência do Poder Judiciário. A etapa de extração da base de dados fundamentou-se na incidência dos seguintes termos: "LGPD"; "proteção de dados pessoais"; "lei de proteção de dados"; e "Lei 13.709", que resultou na coleta de 24.634 documentos. Nesta edição, foi observado um aumento expressivo de decisões coletadas nesta primeira etapa em relação ao ano anterior (15.921 documentos).

Diante disso, a pesquisa passou por uma série de etapas que visam aprimorar a extração automatizada das decisões. Em um primeiro momento, foi disponibilizada pelo Jusbrasil uma amostra de decisões com base em alguns critérios da edição anterior, a qual foi submetida à uma primeira revisão por membros do Cedis/IDP. Nesta fase, foram apresentadas contribuições iniciais, com vistas ao aprimoramento da seleção de decisões. As contribuições concentraram-se no aperfeiçoamento: i) dos critérios de classificação por níveis de relevância; ii) da extração de processos incluídos no escopo da pesquisa - seja em função do lapso temporal, seja em razão da confirmação de que a decisão consistia em sentença ou acórdão; e iii) do mapeamento dos artigos da LGPD mencionados em cada decisão.

Em seguida, a fim de aprimorar de forma mais aprofundada os critérios de compreensão para i) a tipologia da decisão (decisão monocrática, sentença, acórdão, etc), ii) a classificação das decisões por níveis de relevância, bem como iii) o mapeamento de artigos da LGPD citados na decisão, foi selecionado um espaço amostral de 300 decisões selecionadas de forma aleatória para que os pesquisadores voluntários realizassem a revisão por espaço amostral destas informações classificadas e indicadas de forma automatizada.

Os resultados indicaram uma acurácia média de aproximadamente 94%, atestando elevado grau de confiabilidade do processo automatizado na extração de artigos da Lei e classificação de relevância da decisão. A amostra avaliada assegura nível de confiança de 95% e margem de erro de 5,6%¹.

1. O nível de confiança foi definido com base no Escore-z (valor crítico da distribuição normal padronizada), que estabelece o multiplicador estatístico necessário para o grau de certeza desejado. A margem de erro foi calculada com base na Fórmula de Cochran para Proporções, ajustada pelo Fator de Correção para População Finita (FPC).

Adicionalmente, a inteligência artificial foi empregada para extração de variáveis complementares, com acurácia superior a 90%, conforme verificado pelo Jusbrasil. Com as análises dos pesquisadores e a compreensão de padrões de inconsistências pelos membros do Cedis/IDP, foi realizada uma nova seleção amostral de aproximadamente 220 decisões, contando com o refinamento de tais critérios pelas ferramentas de extração de informações das decisões pela IA. Nesta etapa, foram acrescentadas novas colunas de informações sobre as decisões que pudessem ser extraídas pela IA², cujos critérios foram previamente definidos por membros do Cedis/IDP e parametrizados pelo Jusbrasil nos respectivos sistemas de IA. As novas colunas de informações mapeadas pela IA foram avaliadas pelos pesquisadores voluntários, que indicaram as respostas ideais para cada informação coletada pela IA das respectivas decisões, conforme instruções pré-determinadas pela coordenação do Projeto no Cedis/IDP, a fim de padronizar as análises.

As decisões analisadas revisadas foram utilizadas como um conjunto de dados de referência considerado correto e confiável, usado como padrão para avaliar as saídas da IA. Após as alterações com os novos padrões, foram realizados testes de verificação para assegurar a qualidade das saídas e se as inconsistências reportadas eram corrigidas.

Com as novas rodadas de refinamento dos parâmetros a serem coletados pela IA a respeito de cada decisão, concluiu-se por uma base de decisões acompanhada das novas colunas de informações coletadas de forma automatizada. Desta forma, foram mapeadas 5.555 decisões adstritas ao escopo da pesquisa, isto é, que contemplavam, cumulativamente, os 3 critérios: i) ser uma decisão de alta relevância (níveis 3 e 4); ii) tratar-se de decisão com menção expressa a dispositivo da LGPD; e iii) ser uma decisão classificada como sentença ou acórdão.

Assim, as conclusões que são apontadas neste Relatório referem-se às 5.555 decisões que compõem o escopo da pesquisa.

2. Modalidade da demanda; palavras-chave; assuntos de interesse pré-condicionados; ramos do direito; o setor do polo ativo e do polo passivo; menção à ANPD, acompanhada de justificativa específica; e eventual imposição de "penalidade" (determinações ou condenações), com a correspondente justificativa. Além disso, foram mapeados pela IA questões que são consideradas como de grande importância na aplicação da LGPD, quais sejam: princípios da LGPD mencionados e sua justificativa; a identificação de vazamento de dados e a justificativa correlata; as bases legais abordadas e sua justificativa; o exercício de direitos pelo titular e a respectiva justificativa; e a responsabilidade dos agentes de tratamento e a justificativa da discussão sobre responsabilidade.

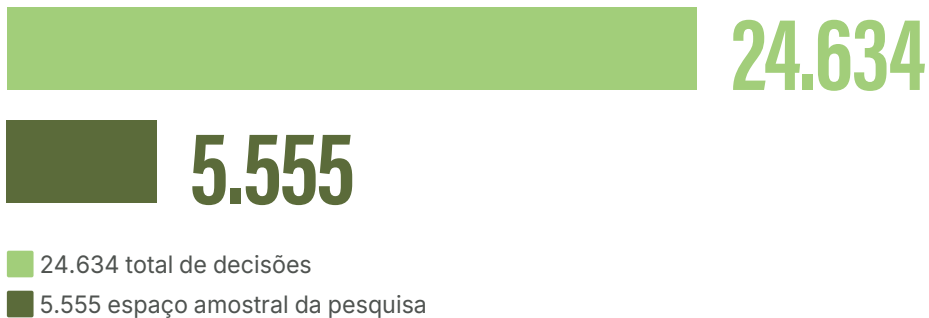


Gráfico 1: Espaço amostral da pesquisa

Nesta 5ª edição, além dos membros do Cedis/IDP e do Jusbrasil, contamos com a participação de 18 pesquisadores voluntários, com diferentes níveis de escolaridade. Na tentativa de traçar uma pluralidade de pesquisadores, a fim de disseminar o conhecimento e discussões sobre LGPD no país, e, igualmente, garantir a tecnicidade das análises realizadas, foram selecionados para participar do projeto pesquisadores pós-graduados e pós-graduandos, graduados e graduandos no final do curso, não limitados aos cursos de Direito – embora a maioria dos participantes tenha a referida área como origem acadêmica ou de atuação. Um dos critérios de escolha para a composição do grupo foi a atuação dos candidatos, de modo a abarcar os setores público e privado, terceiro setor e comunidade científica de diferentes formações acadêmicas e regiões do país.

Assim como na edição anterior, notou-se a necessidade de contar com uma menor quantidade de participantes, a fim de garantir comunicação mais eficaz e melhor direcionamento das análises conduzidas pelos participantes.

As análises dos participantes foram instruídas pelas coordenadoras do Projeto Painel LGPD nos Tribunais 2025-2026 no Cedis/IDP desta edição, Profa. Mônica Fujimoto, Sayuri Hamaoka e Eduarda Costa. Foram realizadas reuniões e explicações para alinhamento metodológico para orientar a forma de revisão das informações extraídas pela IA e à uniformização de critérios de preenchimento, bem como a disponibilização de diretrizes específicas sobre a resposta considerada adequada em cada coluna da planilha. Além disso, os encontros também contaram com a apresentação pelos pesquisadores sobre as decisões a eles designadas, que destacaram padrões das decisões de forma abrangente, de inconsistências extraídas pela IA, bem como de apontamentos de principais temas abordados, setores envolvidos de forma recorrente, níveis de discussão da LGPD no âmbito das decisões e realces a casos e interpretações pontuais. Por

fim, foi solicitado que os pesquisadores enviassem resumos de casos sobre temas e decisões consideradas recorrentes, importantes ou diferenciadas.

A pesquisa foi acompanhada de revisão e aprimoramento contínuo, pela coordenação do Projeto no Cedis/IDP, das diretrizes de preenchimento, a partir da conferência de adequação do preenchimento de revisão realizada pelos pesquisadores voluntários, bem como de dúvidas por eles levantadas. Em paralelo às revisões dos pesquisadores, a coordenação do Projeto no Cedis/IDP também mapeou padrões em que a IA retornava informações de forma inconsistente, as quais eram aprimoradas a cada nova extração realizada, a partir da melhoria de prompts para a IA, operacionalizadas pelo Jusbrasil.

Esta edição do Projeto Painel LGPD nos Tribunais retrata uma integração da inteligência artificial na pesquisa acadêmica atualmente. A junção entre a análise dos pesquisadores voluntários e membros do Cedis/IDP e a extração de informações automatizadas por inteligência artificial, propiciadas pelo Jusbrasil, demonstra a importância de se promover estudos multidisciplinares, que requerem a colaboração de expertises humanas distintas e complementares. Nesta edição, a revisão das informações extraídas das decisões pela IA e a necessidade de se repensar regras para a padronização de resposta no plano macro foram desafios instigantes para o aprimoramento do uso da IA como ferramenta de pesquisa.

Frente a isso, tendo em vista a quantidade de decisões e amplitude de campos extraídos, é possível que, mesmo diante de revisões, aprimoramento de comandos para a IA, bem como da robustez metodológica e analítica desta pesquisa, existam inconsistências não detectadas. Importante também lembrar que os apontamentos deste Relatório refletem as características do espaço amostral selecionado, proveniente de decisões disponíveis publicamente pelo Poder Judiciário.

Diante das notas metodológicas que pavimentam a construção deste Relatório, a partir da exposição do objetivo da pesquisa, as variáveis adotadas, bem como suas limitações, esta pesquisa empírica singular do Painel LGPD nos Tribunais revela a importância de compreender, na prática, as tendências de aplicação da LGPD pelo Judiciário. A pesquisa fomenta a busca pelo contínuo aprimoramento das discussões de proteção de dados pessoais no território brasileiro. A pesquisa, portanto, traz um debate qualificado sobre o tema, difundindo conhecimentos sobre a Lei Geral de Proteção de Dados Pessoais e a sua efetivação.

Ademais, a pesquisa se apresenta como ferramenta de pesquisa àqueles que se dedicam ao entendimento da LGPD no dia a dia e impulsiona a academia a analisar criticamente a aplicação da Lei, bem como a construir uma doutrina sólida dos temas relacionados à proteção de dados pessoais no Brasil.

PAINEL LGPD NOS TRIBUNAIS

2

Raio-X do Painel LGPD 2025

Panorama geral dos processos analisados

Ao longo dessas 5 edições de pesquisa, percebe-se um aumento gradual da quantidade de documentos que mencionam o tema de proteção de dados pessoais. Nesta edição, foram extraídos 24.634 documentos. Veja-se a progressão dos números de documentos coletados em cada uma das edições, desde 2020³:

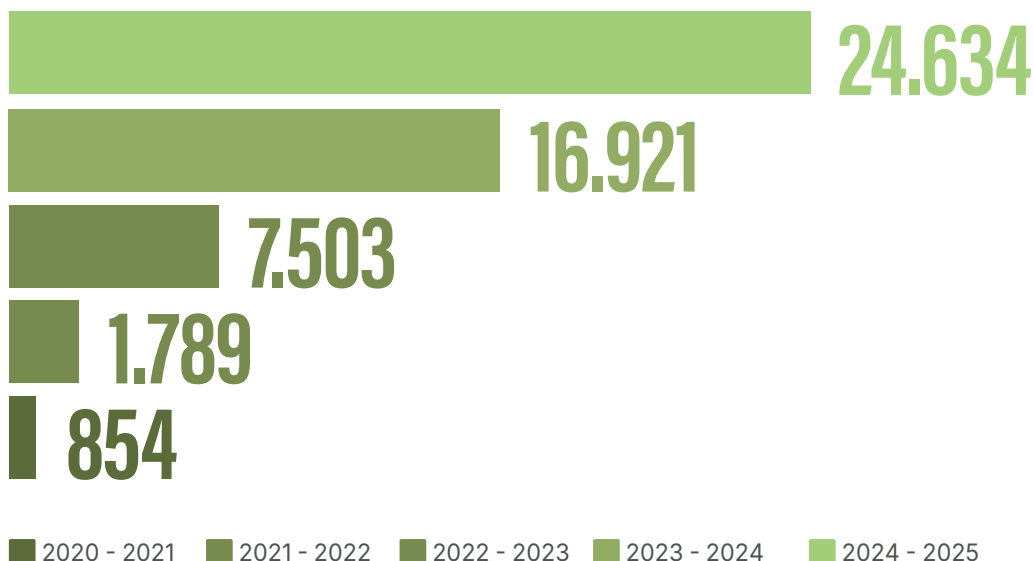


Gráfico 2: número de documentos por ano

3. As edições passadas podem ser acessadas em: <<https://painel.jusbrasil.com.br/>>.

Quanto ao mapeamento de tribunais que mais tiveram decisões a respeito do tema de proteção de dados pessoais em geral, considerando as 24.634 decisões, ressaltam-se aqueles vinculados aos estados de São Paulo, Minas Gerais e Paraná:

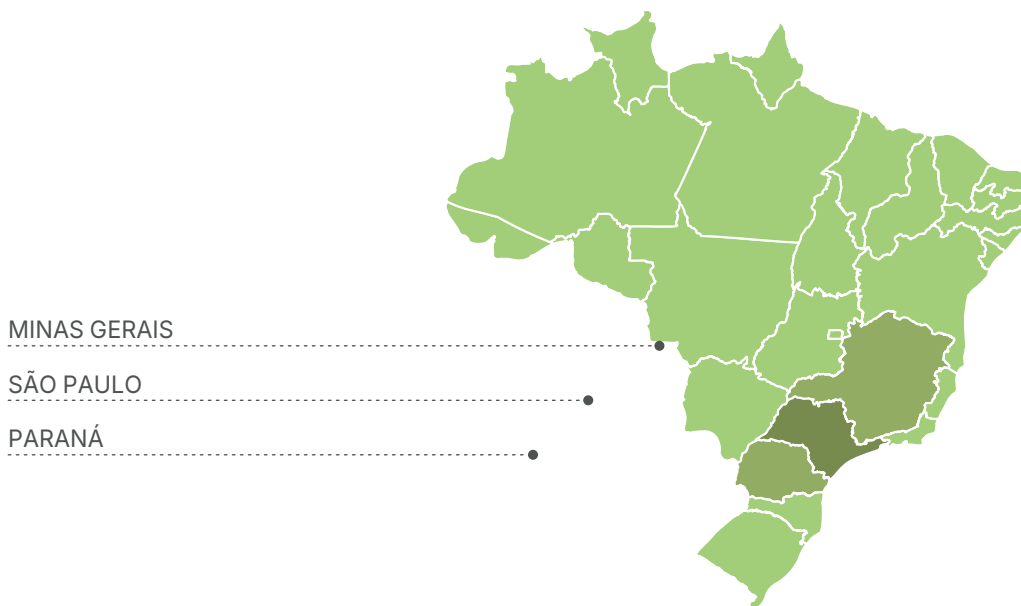


Gráfico 3: concentração de decisões por estados brasileiros

Como também observado nas edições anteriores, percebe-se a concentração em volume de decisões no Tribunal de Justiça de São Paulo (TJSP). Entretanto, em comparação com as duas edições anteriores (3ª e 4ª edições), foi possível observar uma maior pulverização do volume de decisões do TJSP para outros tribunais. Em especial, percebeu-se um aumento nos tribunais Tribunal Regional do Trabalho da 2ª Região (TRT-2) e Tribunal de Justiça de Minas Gerais (TJMG):

Tabela 1: Tribunais com maior número de decisões - Todas as edições

1ª Edição (2020 - 2021)		2ª Edição (2021 - 2022)		3ª Edição (2022 - 2023)		4ª Edição (2023 - 2024)		5ª Edição (2024 - 2025)	
Tribunal	Nº	Tribunal	Nº	Tribunal	Nº	Tribunal	Nº	Tribunal	Nº
TJSP	25%	TJSP	59%	TJSP	43%	TJSP	45%	TJSP	29%
TRT-2	14%	TJBA	7%	TRT-2	7%	TRF-4	10%	TRT-2	16%
TJPR	6%	TJDFT	6%	TRT-3	7%	TJRS	5%	TJMG	9%

TRT-4	5%	TJRS	4%	TRT-4	5%	TJMG	4%	TRT-21	4%
TJMG	5%	TRF-4	3%	TJPR	4%	TJDFT	3%	TJPR	3%
STF	5%	TJRJ	2%	TRT-9	3%	STJ	3%	TRF-4	3%
TRT-3	5%	TJPR	2%	TJDFT	3%	TRT-3	3%	TRT-5	3%
TRT-1	4%	TJMG	2%	TJSC	3%	TRT-9	2%	TJGO	3%
TJDFT	3%	TRT-7	2%	TRT-8	3%	TJPR	2%	TRT-9	2%
TRT-23	2%	TRT-11	1%	TJRJ	2%	TRT-15	2%	TJRO	2%
TRT-10	2%	TRT-4	1%	TRT-12	2%	TRT-2	2%	TRT-23	2%
TST	2%	TST	1%	TJBA	2%	TRT-4	2%	TJCE	1%
TRT-6	2%	TCU	1%	TJMG	1%	TJES	2%	TJRJ	1%
TRT-19	1%	TRT-2	1%	TJRS	1%	TJRJ	1%	TRT-15	1%
TJBA	1%	TRT-12	1%	TRT-13	1%	TJAM	1%	TJDFT	1%
TJRS	1%	TRT-17	1%	TRT-15	1%	TJGO	1%	TJRN	1%
STJ	1%	TJMT	1%	TRF-4	1%	TRT-8	1%	TJMT	1%
TJRJ	1%	TRT-18	1%	TJMS	1%	TST	1%	TRF-3	1%
TRT-21	1%	TSE	1%	TRT-18	1%	TRT-18	1%	TJSC	1%
TJMS	1%	TCE MS	1%	TRT-23	1%	TJSC	1%	TJPA	1%

Nesta 5ª edição, a classificação sobre a relevância das decisões voltou a ser dividida⁴ em 4 níveis, como indicado nas notas metodológicas.

Diferentemente da edição anterior, o nível de relevância foi classificado de forma ampla a todas as 24.634 decisões encontradas, o que inclui àqueles documentos que contemplam todos os tipos de decisões (sejam elas sentenças,

4. Nas edições anteriores, as decisões foram classificadas da seguinte maneira: no primeiro ano de pesquisa (2020 – 2021), o nível de relevância era dividido em: (0) pouco relevante; (1) relevante; (2) muito relevante; e (3) excelente; já no segundo ano (2021-2022), os níveis de relevância foram divididos em (0) não é decisão judicial; (1) não possui relação com a LGPD; (2) apenas menciona a LGPD; (3) a LGPD é debatida de forma importante, mas não é o ponto central do caso; e (4) a LGPD é a questão central do caso; no terceiro ano (2022-2023) os filtros de relevância foram divididos em: (0) não é decisão judicial; (1) não possui relação com a LGPD; (2) apenas menciona a LGPD no relatório; (3) apenas menciona a LGPD sem aprofundamento; (4) debate incidental sobre a LGPD (menção na fundamentação, mas a Lei não é decisiva para o resultado); e (5) a LGPD é a questão central do caso. No quarto ano, os filtros de relevância foram divididos em: (1) não possui debate relevante sobre a LGPD (menção dos artigos apenas no relatório ou mera citação) ou não possui relação com a LGPD; (2) debate incidental sobre a LGPD (menção na fundamentação, mas a Lei não é decisiva para o resultado); e (3) a LGPD é a questão central do caso.

acórdãos, decisões monocráticas, etc) e que não necessariamente mencionam artigos da LGPD. Dentre as 24.634 decisões, 8.709 foram classificadas como de relevância 3 ou 4. Com o objetivo de obtermos conclusões mais significativas sobre as interpretações do tema de proteção de dados pessoais nos tribunais, o escopo desta pesquisa restringe-se às 5.555 decisões que, cumulativamente: i) são de alta relevância (níveis 3 e 4); ii) contêm menção expressa a dispositivo da LGPD; e iii) são classificadas como sentença ou acórdão. Destas decisões adstri-
tas ao escopo da pesquisa:

i) 43,1% são de alta relevância de nível 4, ou seja, aquelas em que a LGPD é a questão central do caso; e 56,9% são de alta relevância nível 3, isto é, aquelas em que há um debate incidental sobre a LGPD, ainda que haja um aprofundamen-
to sobre o tema de proteção de dados, mas ele não seja imprescindível para a resolução da lide:

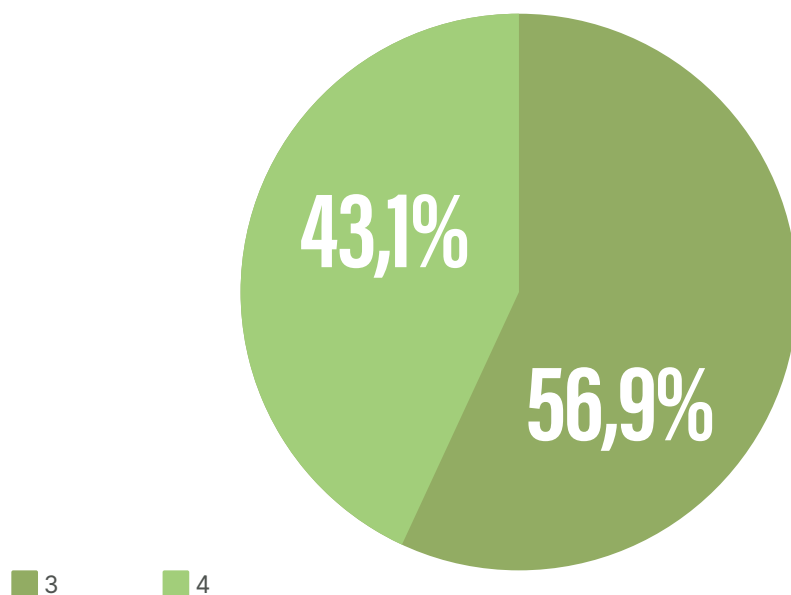


Gráfico 4: Decisões por relevância em porcentagem (níveis 3 e 4)

ii) 29,9% são acórdãos e 70,1% são sentenças:

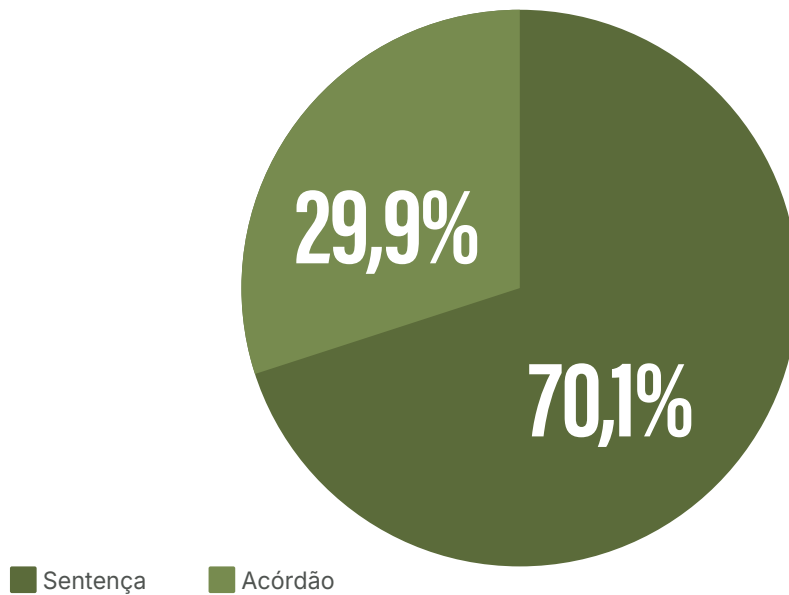


Gráfico 5: Tipo de decisão (entre sentenças e acórdãos)

Destaca-se que todos os mapeamentos que seguem ao longo dos demais tópicos deste Relatório referem-se às decisões adstritas ao escopo da pesquisa, ou seja, às 5.555 decisões mapeadas, conforme critérios supracitados.

PAINEL LGPD NOS TRIBUNAIS

3

Destques Sobre Decisões Relevantes

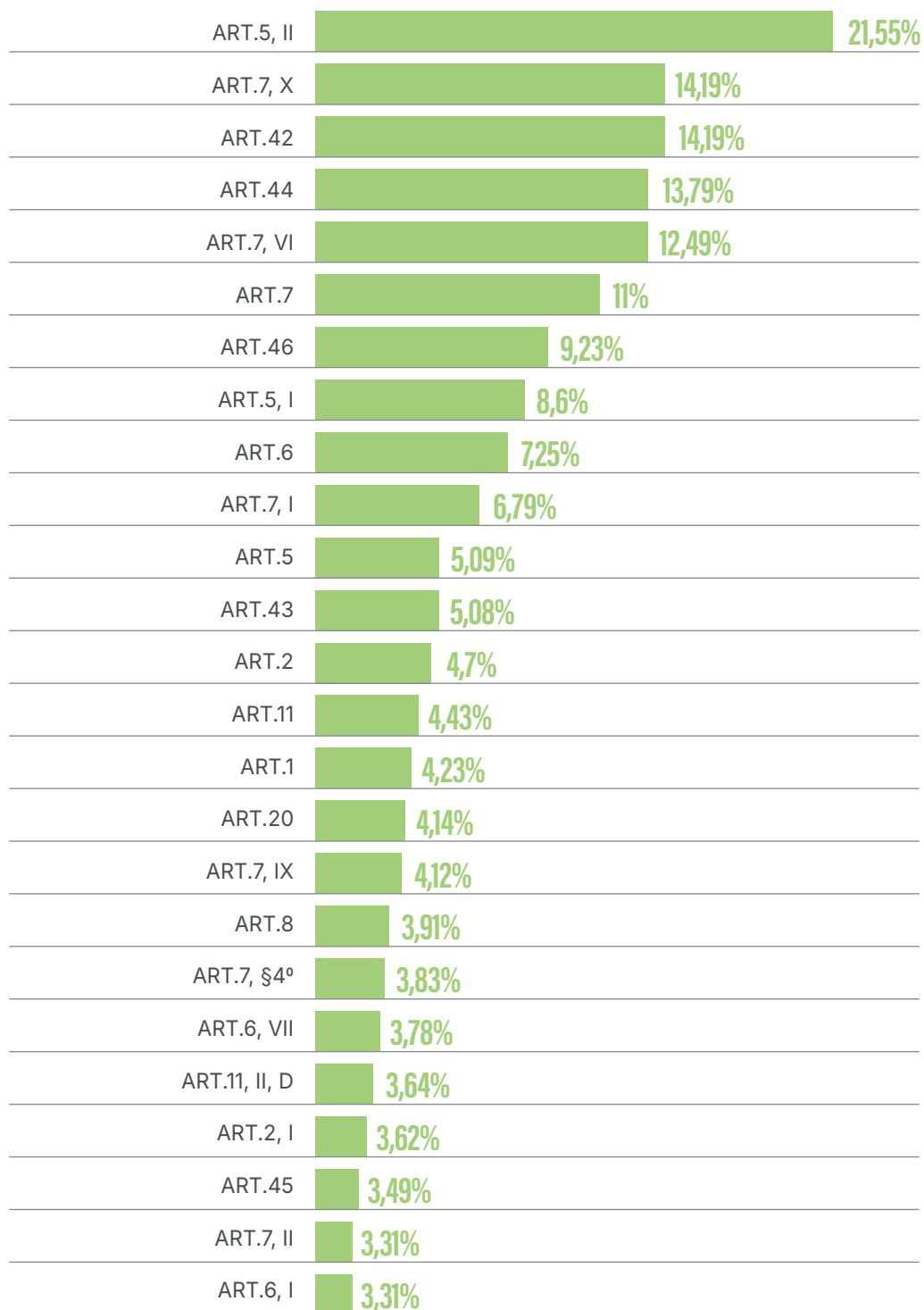
3.1. Menção a artigos da LGPD

O volume crescente de decisões capturadas de forma automatizada relacionadas ao tema de proteção de dados pessoais exigiu que a pesquisa adotasse um recorte mais preciso. Por isso, a menção expressa a dispositivos da LGPD é definida, desde a edição passada, como critério de delimitação do escopo, de forma a restringir as análises à aplicação concreta da LGPD e a compreender os assuntos da Lei que estão sendo abordados nas decisões.

Desta maneira, os artigos da LGPD mais mencionados nas decisões que compõem o escopo da pesquisa foram os seguintes⁵:

5. Os números absolutos e as porcentagens apresentados não representam a contabilização de quantas vezes o artigo é citado, mas sim o número e porcentagem de decisões em que os artigos são citados. Além disso, uma mesma decisão pode mencionar múltiplos artigos da LGPD. As tabelas não apresentam todos os artigos mencionados em decisões. O percentual de corte foi estipulado em 1%, 2%, 2% e 14%, respectivamente, para melhor visualização dos artigos.

Tabela 2: Artigos mais mencionados



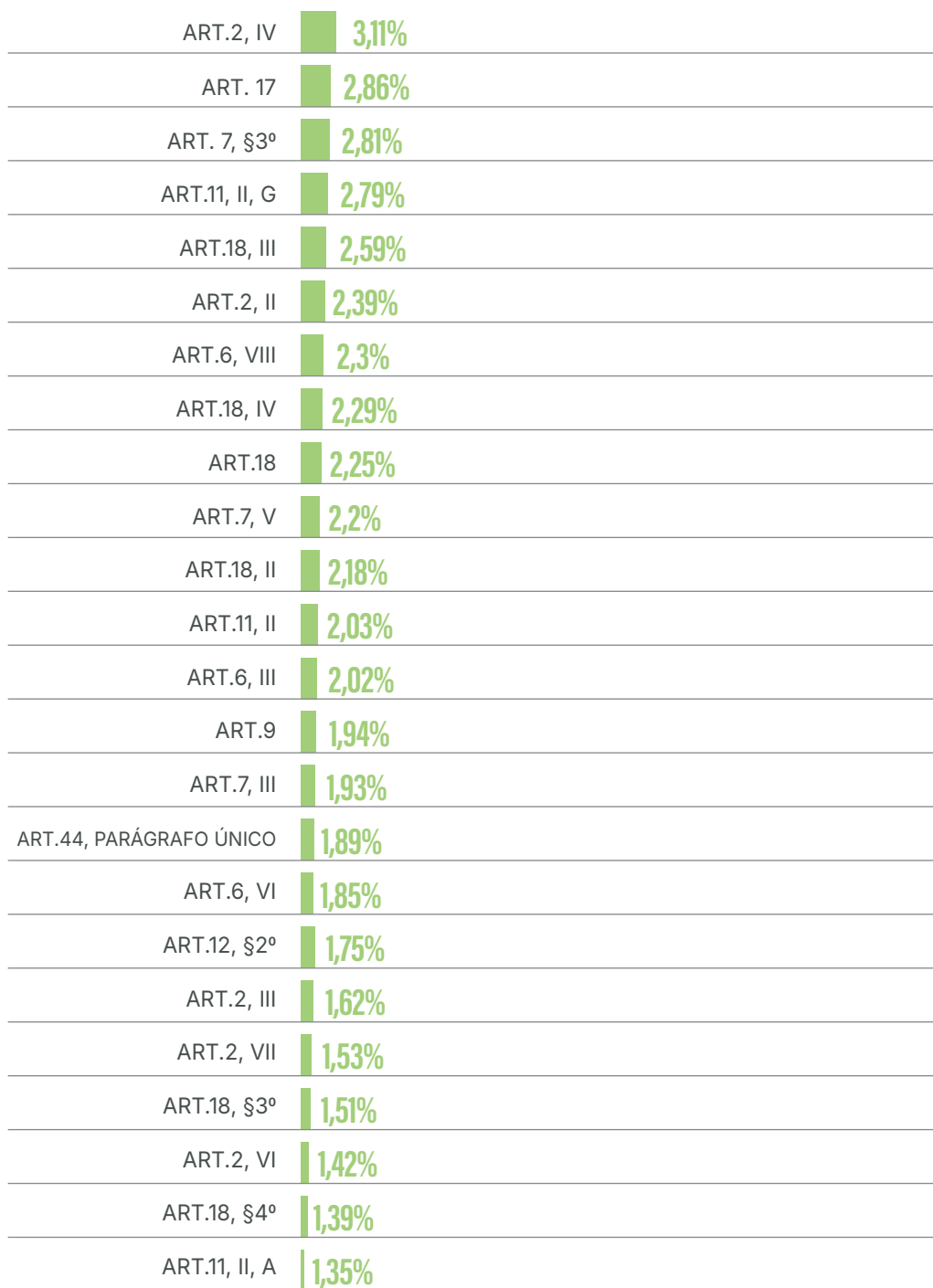
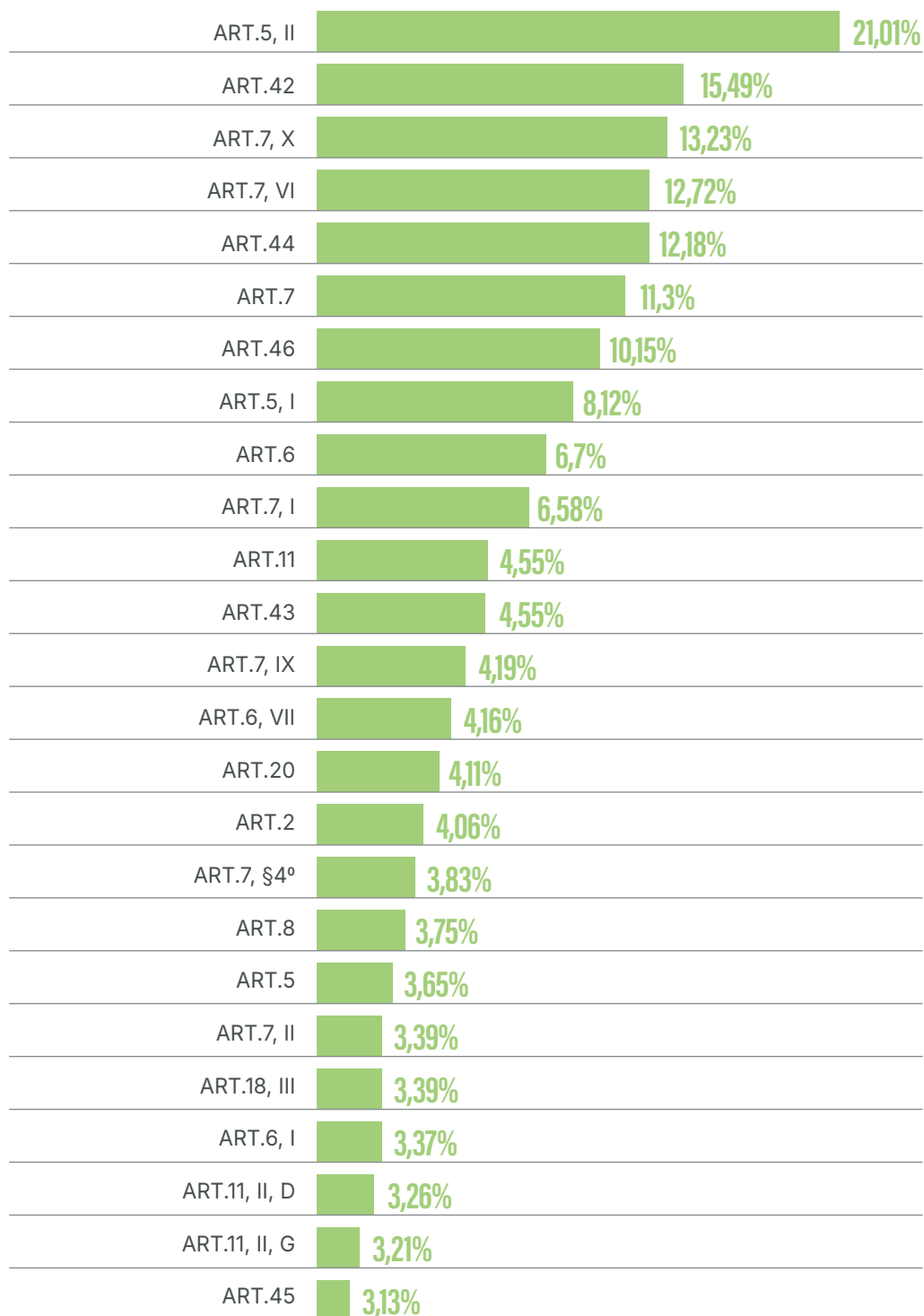


Tabela 3: Artigos mais citados em 1ª instância



ART.2, I	3,03%
ART. 18, IV	2,8%
ART. 7, §3º	2,77%
ART.18, II	2,75%
ART.6, VIII	2,49%
ART.7, V	2,47%
ART.2, II	2,39%
ART.2, IV	2,39%
ART.18	2,31%
ART.6, VI	2,18%
ART.18, §3º	2,11%
ART.1	2,03%

Tabela 4: Artigos mais citados em 2ª instância

ART.5, II	22,82%
ART.44	17,72%
ART.7, X	16,38%
ART.7, VI	11,77%
ART.42	11,23%
ART.7	10,25%
ART.5, I	9,65%
ART.1	9,41%
ART.5	8,56%
ART.6	8,5%
ART.46	7,1%
ART.7, I	7,04%
ART.43	6,31%
ART.2	6,25%
ART.17	5,7%
ART.2, I	4,92%
ART.2, IV	4,85%
ART.45	4,37%
ART.11, II, D	4,37%
ART.20	4,25%
ART.8	4,19%
ART.11	4,07%
ART.7, IX	3,88%
ART.7, §4º	3,76%
ART.4	3,76%

ART.9	3,52%
ART.7, III	3,34%
ART.6, I	3,16%
ART.7, II	3,03%
ART.6, VII	2,91%
ART.7, §3º	2,79%
ART.6, III	2,79%
ART.11, II	2,61%
ART.11, I	2,37%
ART.2, II	2,31%
ART.12, §2º	2,25%
ART.2, III	2,25%
ART.18	2,12%
ART.2, VII	2,12%
ART.2, VI	2,06%

Tabela 5: Artigos mais citados em tribunais superiores

ART.7, VI	35,71%
ART.7, I	35,71%
ART.11, II, D	21,43%
ART.7	21,43%
ART.5, I	21,43%
ART.5, II	21,43%
ART.8	14,29%
ART.9	14,29%
ART.11, II, A	14,29%
ART.11, II B	14,29%
ART.11, II C	14,29%
ART.11, I	14,29%
ART.11, II, E	14,29%
ART.11, II, F	14,29%
ART.11, II, G	14,29%
ART.11	14,29%
ART.7	14,29%
ART.7, §3º	14,29%
ART.7, §4º	14,29%
ART.7, §7º	14,29%
ART.6	14,29%
ART.7, II	14,29%
ART.7, III	14,29%
ART.7, IV	14,29%
ART.7, IX	14,29%







ART.7, V		14,29%
ART.2, I		14,29%
ART.7, VII		14,29%
ART.7, VIII		14,29%
ART.2, II		14,29%
ART.11, II		14,29%

Tabela 6: Quatro artigos mais citados nas decisões

Tema	Artigo	% de decisões
Dado pessoal sensível	ART. 5, II	21,55%
Base legal - proteção do crédito	ART. 7, X	14,19%
Responsabilidade civil e reparação de danos	ART. 42	14,19%
Tratamento irregular de dados	ART. 44	13,79%

Em relação às menções ao artigo 5º, II, da LGPD, ressaltam-se as seguintes tendências:

i. Conceito de dado pessoal e dado pessoal sensível

Paralelo entre dados pessoais sensíveis e "informações sensíveis": o art. 5º, II, da LGPD, é suscitado nas decisões, por diversas vezes, em paralelo ao conceito de informações sensíveis previsto no art. 3º, § 3º, II, da Lei do Cadastro Positivo (Lei nº 12.414/11). Este paralelo é suscitado nas hipóteses que discutem a possibilidade de tratamento de dados pessoais para fins de uso nas práticas de "cadastro positivo" ou credit scoring, que disponibilizam informações ou pontuação a respeito de potencial risco na concessão de crédito ao consumidor⁶.

6. Exemplificativamente: TJAC. 0700015-48.2024.8.01.0012. Juiz: Zacarias Laureano de Souza Neto. Vara Única - Cível da Comarca de Manoel Urbano. Data de Julgamento: 16/06/2025. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/tj-ac/4082103301/inteiro-teor-4082103306> TJSP. 1000617-15.2024.8.26.0094. Relator: Issa Ahmed. 34ª Câmara de Direito Privado. Data de Julgamento: 16/12/2024. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/2939318531>

Conceito de dado pessoal sensível para afastamento de dano moral presumido: o art. 5º, II, da LGPD é evidenciado em casos em que se mencionam a ausência de condenação do agente de tratamento por dano moral presumível, dada a natureza não sensível do dado, seguindo o entendimento exposto no AREsp 2.130.619/SP, julgado pelo STJ em 2023⁷. Em diversos casos, tal tese é suscitada mesmo quando a decisão já reconheceu a inexistência do nexos causal entre o suposto tratamento irregular de dados pelo agente de tratamento e o dano requerido, de modo que o afastamento do dano moral presumido é utilizado como tese de reforço⁸. No entanto, em razão da discussão travada nos autos do REsp 2201694/SP, REsp 2.133.261/SP e REsp 2.115.461/SP⁹, salienta-se que, em caso de dados pessoais tratados por gestores de bancos de dados e disponibilizados a terceiros consulentes, a 3ª Turma do STJ, vem entendendo, por maioria, que tal conduta é apta a gerar dano moral indenizável in re ipsa.

Proteção especial do dado pessoal sensível: em algumas decisões, constata-se a discussão sobre o dado pessoal sensível possuir maior proteção no ordenamento jurídico. Por vezes, afastam-se as teses de que há necessidade de condenação a indenizações em razão da natureza do dado, principalmente quando o dado pessoal não é qualificado como sensível¹⁰.

-
7. Exemplificativamente: TJAL. 0000154-70.2024.8.02.0058. Juíza: Luciana Josué Raposo Lima Dias. Data de Julgamento: 06/05/2025. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/tj-al/3662319849/inteiro-teor-3662320039>; TJPR. 00073240720238160069 Cianorte, Relator.: Alvaro Rodrigues Junior, Data de Julgamento: 13/12/2024, 2ª Turma Recursal, Data de Publicação: 16/12/2024, disponível em: <https://www.jusbrasil.com.br/jurisprudencia/tj-pr/2939243508/inteiro-teor-2939243528>
 8. Exemplificativamente: TJAL. 0000146-93.2024.8.02.0058. Juíza: Luciana Josué Raposo Lima Dias. Data de Julgamento: 28/04/2025. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/tj-al/3549679464/inteiro-teor-3549679483>; TJAM. 0601294-87.2024.8.04.4600. Juíza: Nayara de Lima Moreira Antunes. Data de Julgamento: 15/10/2024. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/tj-am/3865373773/inteiro-teor-3865373780>; TJMG. 50059957720248130567, Relator.: Des. (a) Monteiro de Castro, Data de Julgamento: 15/08/2025, 15ª Câmara Cível, Data de Publicação: 25/08/2025. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/tj-mg/4560349299>
 9. STJ. REsp: 2201694, Relator.: Ministra Nancy Andrighi, Data de Julgamento: 04/11/2025, Data de Publicação: DJEN 04/11/2025, Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/stj/5641692665/inteiro-teor-5641692666>; STJ. REsp: 2133261, Relator.: Ministra Nancy Andrighi, Data de Julgamento: 08/10/2024, T3 - TERCEIRA TURMA, Data de Publicação: DJe 10/10/2024, Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/stj/2939301842>; STJ. REsp: 2115461, Relator.: Ministra Nancy Andrighi, Data de Julgamento: 08/10/2024, T3 - TERCEIRA TURMA, Data de Publicação: DJe 14/10/2024. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/stj/2939383241>
 10. Exemplificativamente: TJSP. 10127081620248260005, Relator.: Antonio Carlos Santoro Filho, Data de Julgamento: 19/02/2025, 1ª Câmara de Direito Privado, Data de Publicação: 19/02/2025, Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/tj-sp/3083652750/inteiro-teor-3083652768>; TRT-2. 10018780720245020717, Relator.: Waldir Dos Santos Ferro, Data de Julgamento: 30/04/2025, 11ª Turma - Cadeira 4, Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/trt-2/3962876611/inteiro-teor-3962876629>

Dado pessoal sensível. Dano presumido afastado. Incidente de dados.

Dispositivos da LGPD citados: ART. 7 | ART. 5, II

Trata-se de ação de indenização por danos morais por ocorrência de incidente cibernético que resultou na perda de dados pessoais do titular controlados pela ré.

Discute-se a possibilidade de reparação por danos morais decorrentes de tratamento irregular. Houve notificação do incidente pela ré à titular. Na hipótese, houve divergência de entendimentos quanto à incidência da LGPD ou do CC para fins de aplicação da indenização pelo dano moral. A tese vencedora consistiu no entendimento de que o vazamento ou uso indevido de dados pessoais comuns não configura, por si só, dano moral presumido, nos termos do AREsp 2.130.619/SP, julgado no STJ.

Conforme citado pela decisão, tendo o titular afirmado a ocorrência de dano presumido, sem apontar, no entanto, o prejuízo efetivo, o pleito foi desprovido.

TJMT. 10719263820238110001, Relator.: Antonio Veloso Peleja Junior, Data de Julgamento: 07/10/2024, Segunda Turma Recursal, Data de Publicação: 10/10/2024. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/2891225462>

ii. Base legal da proteção ao crédito

O segundo artigo mais citado nas decisões refere-se ao art. 7º, X, que diz respeito à hipótese legal da proteção do crédito. Esta hipótese legal é transversal a outros tópicos deste Relatório, em especial o relacionado a bases legais e à responsabilidade.

A hipótese legal de proteção ao crédito é frequentemente citada no setor de bancos de dados e no setor financeiro. Os temas mais recorrentes nas decisões são relacionados i) à inscrição de dados pessoais em bancos de proteção ao crédito, para fins de subsidiar serviço de concessão crédito para consumidores, bem como para negociação de dívidas¹¹, e ii) ao compartilhamento dos dados entre instituições financeiras em razão da cessão de crédito entre instituições¹².

A discussão do tratamento de dados por bancos de dados com fundamento na hipótese legal de proteção ao crédito tem sido reiteradamente submetida ao crivo do STJ. Em 2025, no julgamento do REsp 2201694/SP, a Corte consignou, por maioria, que “informações cadastrais e de adimplemento da pessoa cadastrada” não poderiam ser disponibilizadas sem prévio e expresse consentimento do titular, de modo a afastar o uso do art. 7º, X, da LGPD de forma irrestrita, devendo ser lido em conformidade com a Lei nº 12.414/2011 (art. 4º, IV, b). Foi decidido, ainda, que tal compartilhamento ensejaria dano moral in re ipsa. Tal posicionamento seguiu o entendimento adotado no REsp 2.133.261/SP e REsp 2.115.461/SP, relatados pela Min. Nancy Andrighi e julgados pela Terceira Turma.

No entanto, o Min. Villas Bôas Cueva e o Min. Humberto Martins, ressaltaram a possibilidade de o art. 7º, X, da LGPD enquadrar-se como fundamento legal para tratamento e disponibilização de dados cadastrais não sensíveis a terceiros consulentes, independentemente do consentimento do titular, uma vez que o serviço oferecido está relacionado à proteção do crédito. Nesse sentido, destacou-se que a proteção do crédito “não implica exclusivamente a análise do risco de crédito, mas se mostra relevante também na obtenção de informações destinadas à identificação do consumidor e aferição de sua real identidade, evitando-se, por exemplo, confusão entre pessoas homônimas e mesmo como um meio de evitar fraudes e para prevenção e mitigação de risco”. Tal posicionamento também foi ressaltado pelo Min. Villas Bôas Cueva nos autos do REsp 2.115.461/SP. Nas decisões selecionadas para o escopo da pesquisa nesta edição, verificou-se que o entendimento firmado, por maioria, pela Terceira Turma do STJ, tem sido acolhido de forma minoritária nos demais tribunais nacionais, embora em quantidade já significativa.

Uma discussão interessante que ainda está pendente de julgamento pelo

-
11. Exemplificativamente: TJSP. 10003545120248260233 Ibaté, Relator.: Claudia Menge, Data de Julgamento: 21/01/2025, 32ª Câmara de Direito Privado, Data de Publicação: 21/01/2025. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/tj-sp/3004765849/inteiro-teor-3004765853>; TJRJ. 08361449620238190205 202500118057, Relator.: Des(a). Cintia Santarem Cardinali, Data De Julgamento: 16/04/2025, Quinta Câmara De Direito Privado (Antiga 24ª Câmara Cível), Data de Publicação: 29/04/2025. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/tj-rj/3552120801/inteiro-teor-3552120828>
 12. Exemplificativamente: TJ-SP. 10140272820248260002, Relator.: Fernando Sastre Redondo, Data de Julgamento: 04/11/2024, 38ª Câmara de Direito Privado, Data de Publicação: 04/11/2024. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/tj-sp/2827898232> TJ-SP. 10660756120248260002 São Paulo, Relator.: Simões de Almeida, Data de Julgamento: 21/03/2025, 13ª Câmara de Direito Privado, Data de Publicação: 21/03/2025, Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/tj-sp/3294869245/inteiro-teor-3294869272>

STJ refere-se à definição sobre a dívida prescrita poder ser exigida extrajudicialmente, inclusive com a inscrição do nome do devedor em plataformas de acordo ou de renegociação de débitos. Nos autos do IRDR do TJMG¹³, este tópico foi discutido à luz da LGPD em relação à alteração de hipótese legal após a dívida passar a ser prescrita, tratando da eventual (im)possibilidade de alternar-se o tratamento que antes era lícitamente realizado com base na proteção ao crédito (art. 7º, X) para passar a fundamentar-se no consentimento (at. 7º, I).

IRDR. Bases legais do tratamento. Consentimento. Proteção ao crédito. Dívida prescrita

Dispositivos da LGPD citados: ART. 7º, I | ART. 7º, X.

Trata-se de IRDR instaurado no TJMG para definir se a inclusão de débito prescrito em plataformas de negociação de dívidas (classificadas no setor de bancos de dados) configura ato ilícito e se essa conduta é apta a gerar dano moral.

A discussão a respeito da LGPD foi suscitada em um dos Votos, oportunidade em que se problematiza a permanência do tratamento de dados relativos à dívida prescrita com fundamento na hipótese legal de proteção ao crédito. A tese apontada foi a de que, uma vez prescrita a dívida, a base legal de proteção do crédito (art. 7º, X) seria inaplicável, pois os dados deixariam de ser necessários para a finalidade originária (proteção ao crédito); por isso, a continuidade do tratamento na plataforma dependeria, em tese, de consentimento do titular (art. 7º, I).

Foi instaurado o incidente, com a suspensão dos feitos sobre o tema no estado. A controvérsia também está submetida ao STJ no Tema Repetitivo 1264, afetado para definir se a dívida prescrita pode ser exigida extrajudicialmente, inclusive com inscrição do nome do devedor em plataformas de acordo ou renegociação.

TJMG - IRDR: 18444264420228130000, Relator.: Des .(a) Pedro Bernardes de Oliveira, Data de Julgamento: 28/08/2024, 2ª Seção Cível, Data de Publicação: 02/10/2024, Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/tj-mg/2772422293/inteiro-teor-2772422298>

13. Ao fim deste tópico, destaca-se o resumo dos argumentos suscitados em um dos votos do IRDR. TJ-MG - IRDR: 18444264420228130000, Relator.: Des .(a) Pedro Bernardes de Oliveira, Data de Julgamento: 28/08/2024, 2ª Seção Cível, Data de Publicação: 02/10/2024, Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/tj-mg/2772422293/inteiro-teor-2772422298>

iii. Responsabilidade, reparação de danos e Tratamento irregular de dados

O art. 42 e 44 são artigos discutidos em diversas decisões, acerca de diversos setores e tópicos em geral, e demonstrando a tendência de que a responsabilidade tem se consolidado como tema central nas discussões travadas perante os tribunais quanto à proteção de dados pessoais.

As decisões têm consolidado os arts. 42 e 44 como dispositivos centrais nas discussões de responsabilidade e incidentes de segurança. O art. 42 é mencionado em quase 15% das decisões totais (5.555) e tem sido aplicado de forma consistente nos casos em concreto, tanto para o reconhecimento quanto para o afastamento da responsabilidade. O art. 44, por sua vez, tem alta aplicação nos casos de incidentes de segurança. Sua incidência tem sido muito disseminada em razão do REsp n. 2.077.278/SP, julgado em 2023 pela 3ª Turma do STJ.

Ambos os artigos são majoritariamente mencionados nas decisões que apuram os pressupostos da responsabilidade civil, quais sejam, o ato ilícito, o dano e o nexo causal, e são frequentemente citados em paralelo com a responsabilidade objetiva de relações de consumo, prescindindo de análise de culpa. Tanto o art. 42 quanto o art. 44 são regularmente abordados em paralelo ou em conjunto com o art. 14 do CDC, que dispõe sobre a responsabilidade objetiva no contexto consumerista.

Responsabilidade. Ausência de prova do vazamento de dados. Instituição financeira. Empréstimo consignado. Consentimento do titular.

Dispositivos da LGPD citados: ART. 6º, I | ART. 6º, VI | ART. 6º, VII | ART. 1º | ART. 21 | ART. 26, §1 | ART. 27 | ART. 42 | ART. 43 | ART. 44 | ART. 45

Trata-se de caso em que o titular requereu um empréstimo, que dependia de compartilhamento de dados com o INSS, meio de viabilizar a concretização do empréstimo, o qual foi precedido de consentimento do mutuário. Entretanto, o autor foi vítima de golpe, por contratação de empréstimo em outra instituição bancária em seu nome. Alegou-se a existência de vazamento de dados entre instituições e a necessidade de ser indenizado pelos danos.

O colegiado destacou que a LGPD, conforme o art. 1º, visa à proteção da privacidade e dos direitos fundamentais, mas não afasta a necessidade de prova do nexo causal. Foram invocados os princípios da finalidade, transpa-

rência e segurança previstos no art. 6º, I, VI e VII, cuja violação não restou comprovada.

O acórdão ressaltou que é vedado, expressamente, no § 1º, do art. 26, que o Poder Público transfira, às entidades privadas, dados pessoais constantes de suas bases de dados, salvo quando houver previsão legal ou quando a transferência for respaldada em contratos, convênios ou instrumentos congêneres. Além disso, ressaltou-se que, por regra geral, o uso compartilhado de dados é sempre precedido do consentimento do titular dos dados, nos termos do art. 27 da LGPD. Também foi mencionado o art. 21, que veda o uso de dados em prejuízo do titular.

Entretanto, no tocante à responsabilidade civil, a decisão aplicou os arts. 42 a 45 da LGPD, exigindo demonstração concreta do dano e do vínculo com o agente de tratamento, o que não foi demonstrado no caso concreto. A Corte concluiu que não houve prova de vazamento imputável à instituição financeira. Assim, afastou-se o dever de indenizar, reconhecendo a improcedência do pedido.

TRF-4. 5004126-09.2022.4.04.7107/RS, Relator Desembargador Federal Luís Alberto D'Azevedo Aurvalle, 4ª Região, Data de Julgamento: 09/10/2024, Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/trf-4/3594300515/inteiro-teor-3051460800>

3.2. Principais setores envolvidos

Nesta 5ª edição, os setores mais recorrentes do polo ativo foram pessoas físicas, associações e sindicatos e setor privado em geral.

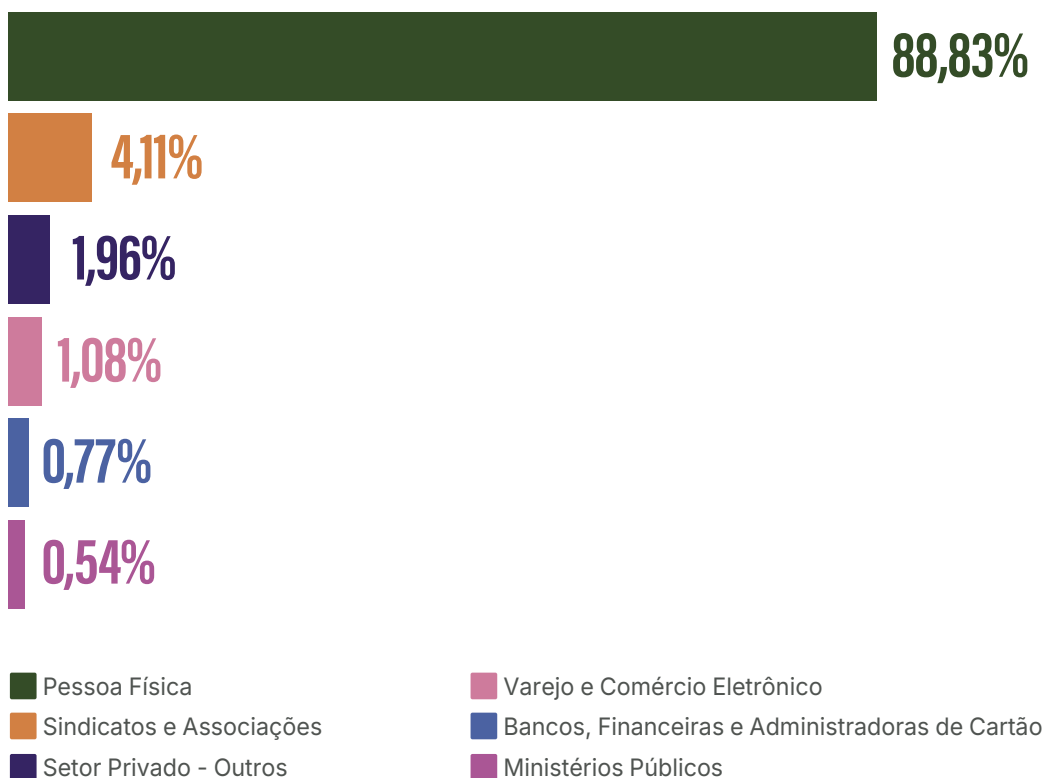


Gráfico 6: Setores mais frequentes – Polo ativo

Quanto ao polo passivo, os setores mais frequentes foram o setor financeiro (bancos, financeiras e administradoras de cartão), bancos de dados (bancos de dados, de cadastros, e empresas de recuperação de crédito) e provedores de conteúdo e outros serviços na internet:

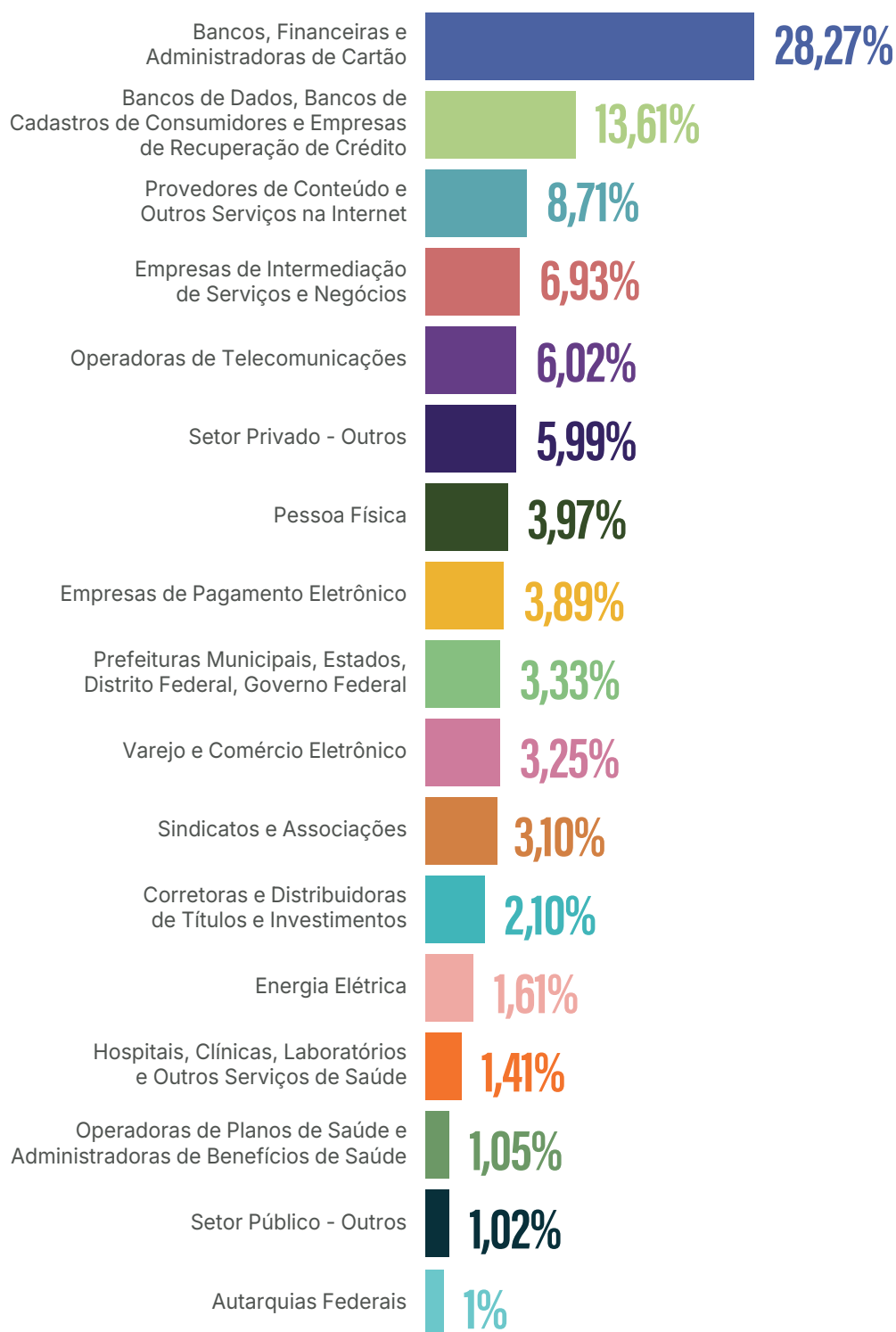


Gráfico 7: Setores mais frequentes – Polo passivo

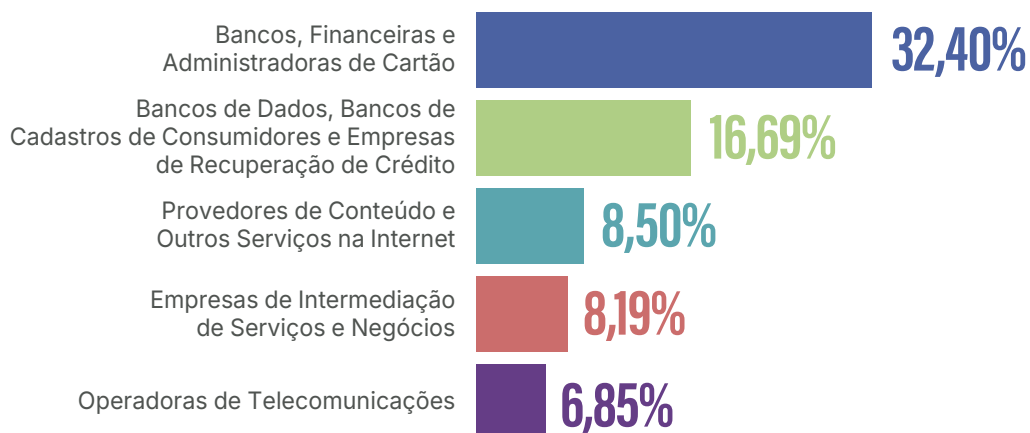


Gráfico 8: Setores mais frequentes polo passivo - 1ª instância

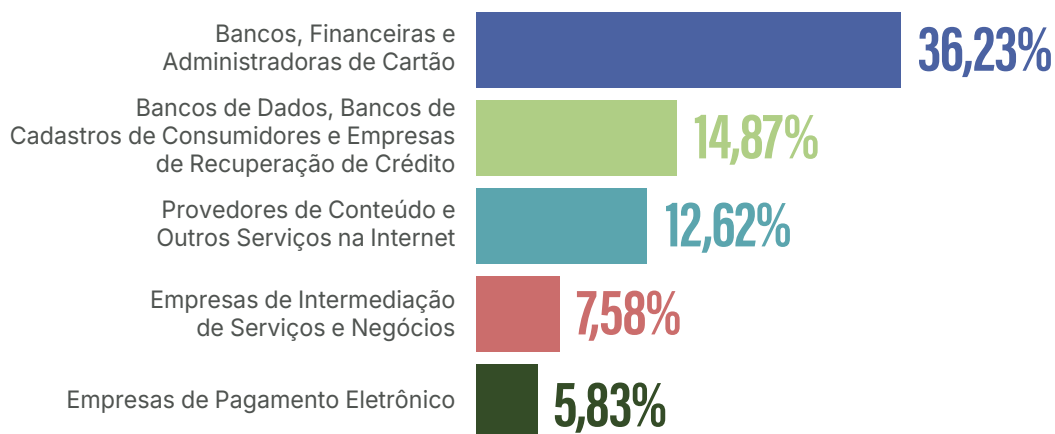


Gráfico 9: Setores mais frequentes polo passivo - 2ª instância e tribunais superiores

Os setores econômicos mais frequentemente mencionados nas decisões analisadas serão citados ao longo das seções deste Relatório de forma específica. A organização do relatório buscou refletir a própria distribuição temática observada no conjunto das decisões, razão pela qual os setores mais recorrentes também aparecem com maior destaque nos diferentes tópicos analíticos.

Assim, setores como: instituições financeiras, bancos de dados, de cadastros e empresas de análise ou recuperação de crédito, provedores de conteúdo e outros serviços na internet, bem como empresas de intermediação de serviços e negócios, por exemplo, tendem a aparecer com maior frequência em determinados tópicos justamente porque grande parte das decisões analisadas envolve controvérsias relacionadas às atividades desempenhadas por esses agentes.

3.3. Ramos do direito correlatos à proteção de dados pessoais

Conforme mencionado anteriormente, um dos questionamentos que direciona esta pesquisa é a compreensão de como a LGPD dialoga com outras disciplinas do Direito. Percebe-se que, em todas as edições, a proteção de dados pessoais perpassa por diversas áreas do Direito, reafirmando a compreensão da proteção de dados como um direito fundamental (art. 5º, LXXIX, da CF). Neste ano, com o auxílio de ferramentas de inteligência artificial, foi realizado o mapeamento das áreas do Direito a partir da identificação dos ramos jurídicos aplicáveis à decisão de forma geral. Assim, cabe suscitar que o Direito Processual Civil é o ramo discutido preliminarmente em diversas decisões, de modo que sua indicação é recorrente, mas não é predominantemente discutido como tópico central das decisões ou em correlação com o tema de proteção de dados.

Diante disso, embora a referida área seja uma das mais abordadas, como se observa da tabela abaixo, optou-se por destacar, dentre as áreas do direito que são abordadas como ramo central da decisão ou em paralelo à proteção de dados, as seguintes áreas: Direito Civil, Direito do Consumidor e Direito do Trabalho¹⁴.

14. Uma mesma decisão pode mencionar múltiplos ramos do direito.

Tabela 7: Principais ramos do direito das decisões

Principais ramos	Decisões analisadas	% de decisões
Direito Civil	4.592	82,66%
Direito Processual Civil	3.792	68,3%
Direito do Consumidor	3.772	67,9%
Direito do Trabalho	858	15,45%
Direito Constitucional	592	10,66%

i. Direito Civil

Considerando as decisões que apresentam Direito Civil como um dos ramos predominantes em discussão, os artigos da LGPD mais frequentemente mencionados em tais decisões são os seguintes:

Tabela 8: Direito Civil - Artigos mais mencionados

Temas	Decisões analisadas	% de decisões
ART. 5 II	1.073	23,37%
ART.42	769	16,75%
ART. 7, X	751	16,35%
ART. 44	745	16,22%

A análise das decisões judiciais indica uma forte intersecção entre as matérias classificadas como Direito Civil e Direito do Consumidor. Constatou-se que aproximadamente 80% das decisões enquadradas em Direito Civil também foram classificadas como relacionadas ao Direito do Consumidor. Além disso, observou-se também que parte das decisões não classificadas como pertencentes ao Direito do Consumidor apresentava, na prática, relações consumeristas. Em muitos casos, os litígios envolviam consumidores e relações típicas consumeristas. Em parte das decisões, o CDC não foi expressamente mencionado, o que pode ter contribuído para a ausência de sua classificação no ramo de "Direito do Consumidor".

Esse aspecto evidencia que parcela significativa das controvérsias envolvendo a LGPD surge no contexto de relações de consumo, mesmo quando classificadas no ramo de Direito Civil^{15 16}.

O tema de Direito Civil envolve, em sua maioria, litígios que dizem respeito aos setores mais frequentemente mencionados em geral, quais sejam: as empresas de bancos de dados, instituições financeiras e provedores de conteúdo ou serviços digitais. Entretanto, ao segmentar o tema de forma mais estrita, a fim de apartar os debates afetos também ao direito do consumidor, observou-se a presença de outros atores: Autarquias Federais (em especial o INSS), Prefeituras Municipais, Estados, Distrito Federal, Governo Federal, bem como Empresas de Intermediação de Serviços e Negócios (o que inclui empresas de transporte de pessoas e de entregas de produtos).

Quanto às temáticas e dispositivos mais recorrentes, o dispositivo da LGPD mais mencionado nas decisões classificadas no campo do Direito Civil foi o artigo 5º, II.

O art. 5º, II é utilizado de forma transversal nas decisões, especialmente para delimitar a natureza das informações discutidas no processo e orientar a análise sobre a aplicabilidade do dano presumido, em caso de haver dados pessoais sensíveis, como já apontado no tópico prévio e como será melhor abordado no tópico de responsabilidade.

Já o art. 7º, X, terceiro artigo mais recorrente, que prevê a proteção ao crédito como hipótese legal de tratamento de dados pessoais, aparece predominantemente em decisões envolvendo bancos de dados e sistemas de análise de crédito e instituições financeiras. Nessas hipóteses, discute-se a legitimidade do tratamento de dados para subsidiar avaliações de crédito por terceiros, cadastrar consumidores em cadastros de negociação, cadastros positivos e de inadimplentes, bem como para o compartilhamento de dados entre instituições quando da cessão de crédito, temas recorrentes nas decisões analisadas ao longo do Relatório.

15. Exemplificativamente: TJ-SP - Apelação Cível: 10016627120228260596 Serrana, Relator: Elói Estevão Trolly, Data de Julgamento: 18/02/2025, 15ª Câmara de Direito Privado, Data de Publicação: 18/02/2025. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/3082771316>

16. Exemplificativamente: TJ-SP - Apelação Cível: 10041407220248260405 Osasco, Relator: Fernando Sastre Redondo, Data de Julgamento: 03/10/2024, 38ª Câmara de Direito Privado, Data de Publicação: 03/10/2024. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/tj-sp/2773339416/inteiro-teor-2773339420>

Apesar da intersecção com o Direito do Consumidor, a temática do Direito Civil nas decisões analisadas não se limita às relações de consumo. Assim como verificado em edições anteriores do relatório, o campo de Direito Civil apresenta abrangência mais ampla, contemplando diferentes tipos de controvérsias relacionadas ao tratamento de dados pessoais.

Seguindo a lógica de artigos mais citados nas decisões, as decisões nesta área do direito frequentemente discutem responsabilidade civil decorrente do tratamento inadequado de dados pessoais, fundamentadas nos arts. 42 e 44 da LGPD, que disciplinam a responsabilização e a reparação de danos, bem como o tratamento irregular de dados.

Entre as demandas recorrentes, destacam-se as discussões envolvendo responsabilidade civil por danos decorrentes do uso indevido de dados, exposição ou compartilhamento irregular de informações pessoais e tratamento de dados em contextos contratuais diversos. Há uma grande quantidade de casos que discutem a responsabilidade de plataformas de intermediação quanto ao bloqueio de contas.

Ressaltam-se, igualmente, os casos do poder público, que dizem respeito ao vazamento de dados, compartilhamento com terceiros sem autorização ou uso indevido em processos judiciais de dados pessoais, com evidência a dados pessoais sensíveis.

Além disso, a questão do dever de publicidade que atinge o poder público em paralelo à proteção de dados pessoais também é discutida, reconhecendo-se muitas vezes a responsabilidade do poder público pela divulgação desnecessária de dados pessoais. Entretanto, há, igualmente, decisões que consideraram a publicidade inerente a certos atos administrativos, afastando a ilicitude do tratamento pelo poder público.

Quanto aos casos de Autarquias (INSS, predominantemente), ressalta-se que a responsabilidade foi aprofundada nos tópicos de responsabilidade e incidentes de segurança de forma exaustiva, de forma que cabe aqui mencionar apenas que as decisões tendem a reconhecer e a destacar a necessidade de se investigar a responsabilidade do INSS quanto à proteção de dados dos titulares, dados os vazamentos de dados recentes.

Rede social. Desativação de conta. Tratamento irregular de dados pessoais. Segurança. Acesso aos dados. Danos morais.

Dispositivos da LGPD citados: ART. 6º, CAPUT E VII | ART. 18, II | ART. 44.

Trata-se de ação movida por titular em face de rede social, em razão da desativação e sem justificativa de perfil profissional, utilizado como ferramenta de trabalho na área da educação. O autor pleiteou a reativação da conta, indenização por danos morais e, subsidiariamente, o acesso integral a todos os dados pessoais armazenados na plataforma.

No tocante à LGPD, o Juízo fundamentou que o tratamento de dados pessoais deve observar a boa-fé e os princípios previstos no art. 6º da LGPD, com destaque para o princípio da segurança (art. 6º, VII). Com base no art. 44 da LGPD, o Juízo entendeu que o cancelamento sumário e injustificado da conta configurou tratamento irregular de dados pessoais, pois não observou a legislação aplicável nem forneceu a segurança que o titular podia legitimamente esperar.

A sentença também reconheceu o direito de acesso aos dados pessoais (art. 18, II, da LGPD), determinando que a ré disponibilizasse ao autor, o acesso integral a todos os dados, arquivos, fotos, vídeos, mensagens e demais informações vinculados à conta, em formato digital legível.

Confirmou-se a tutela de urgência para que a conta fosse reativada, condenou a ré ao pagamento de indenização por danos morais e à disponibilização integral dos dados pessoais do autor.

TJSP. 1002237-30.2024.8.26.0040. Juiz: Daniel Romano Soares. 1ª Vara. Data de Julgamento: 04/06/2025. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/tj-sp/4009499153/inteiro-teor-4009499157>

Tratamento irregular de dados de motorista. Gerenciadora de riscos. Banco de dados. Negativa de carregamento. Exigência abusiva de certidões. Violação à LGPD. Danos morais.

Dispositivos da LGPD citados: ART. 2º, I, II, IV E VII | ART. 6º, I, II, III, V, VII, VIII E IX | ART. 7º, I, II, V | ART. 7º, §3º | ART. 9º, IV E V | ART. 11 | ART. 18, II, III E VII | ART. 42 | ART. 43.

Trata-se de recurso inominado interposto por motorista de caminhão contra sentença que julgou improcedente pedido de indenização por danos morais formulado em face de empresa gerenciadora de riscos no transporte

de cargas. O reclamante alegou estar sendo impedido de realizar carregamentos em razão de inscrição em cadastros internos de restrição mantidos pela ré, que fornece informações às seguradoras de carga, sendo informado de que a recusa decorria de ter sido vítima de assalto em 2017.

A decisão afastou a incidência do CDC, mas reconheceu a plena aplicabilidade da LGPD. Com fundamento no art. 42, §2º, da LGPD, inverteu o ônus da prova em favor do titular.

No mérito, a Turma entendeu que a empresa realizou tratamento de dados do autor de maneira irregular, especialmente ao efetuar pesquisa de antecedentes criminais sem base legal, extrapolando as exigências da Circular nº 422 da SUSEP e da Lei 11.442/2007. A decisão analisou as bases legais do art. 7º da LGPD, concluindo que nenhuma autorizava o tratamento realizado, reconhecendo também violação ao art. 7º, §3º, quanto ao tratamento de dados de acesso público sem observância da finalidade, boa-fé e interesse público.

Comprovadas as negativas de carregamento, à exigência indevida de certidões de antecedentes para poder trabalhar, bem como informações inverídicas ou desatualizadas após verificação junto à Justiça Federal sobre processos do titular, a Turma reconheceu violação aos princípios da finalidade, adequação, necessidade, qualidade dos dados, segurança, prevenção e não discriminação (art. 6º, I, II, III, V, VII, VIII e IX), bem como aos fundamentos da autodeterminação informativa, respeito à intimidade, inviolabilidade da honra e imagem e dignidade (art. 2º, I, II, IV e VII).

Também constatou afronta aos direitos do titular previstos nos arts. 9º e 18 da LGPD, incluindo o direito de acesso, correção de dados inexatos e informação sobre compartilhamento.

Com base no art. 42 da LGPD e diante da ausência de comprovação das excludentes do art. 43, a Turma condenou a empresa ao pagamento de indenização por danos morais.

TJPR. 0005267-24.2023.8.16.0131, Relator Juiz: Fernando Swain Ganem, 3ª Turma Recursal dos Juizados Especiais, Data de Julgamento: 28/03/2025, Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/tj-pr/3359120973/inteiro-teor-3359120977>.

Dado pessoal sensível. Documento médico. Vazamento para terceiro.
Dano moral. Poder Público.

Dispositivos da LGPD citados: ART. 2º, I | ART. 5º, II | ART. 16 | ART. 42

Trata-se de recurso inominado contra sentença de improcedência em ação de indenização por danos morais movida em face de uma Prefeitura Municipal. A autora alegou que documento médico de sua titularidade foi entregue a terceiro, o qual passou a importuná-la com mensagens desagradáveis, configurando violação à sua privacidade e à LGPD.

A Turma Recursal deu provimento ao recurso, fundamentando a decisão na LGPD. O acórdão destacou que a proteção à vida privada é direito fundamental (art. 5º, X, da CF), direito de personalidade (art. 21 do CC) e fundamento da própria LGPD, que elenca o respeito à privacidade como um dos seus pilares (art. 2º, I).

A decisão enquadrou o documento médico como dado pessoal sensível, nos termos do art. 5º, II, da LGPD, que classifica como sensível o dado referente à saúde, sem restrição quanto ao seu conteúdo específico. Ressaltou que dados sensíveis exigem atenção redobrada para evitar vazamentos e que o art. 16 da LGPD prevê a eliminação dos dados após o término de seu tratamento.

O Tribunal entendeu que a entrega de documento médico a terceiro viola a LGPD e ofende direito de personalidade, gerando direito à indenização por dano moral. Com base no art. 42 da LGPD, condenou a Prefeitura ao pagamento danos morais.

TJSP. 1042956-17.2024.8.26.0602, Relator Juiz: Fábio Fresca, 4ª Turma Recursal de Fazenda Pública, Data de Julgamento: 02/04/2025, Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/tj-sp/3350319379/inteiro-teor-3350319381>

ii. Direito do Consumidor

Quanto às decisões que abordaram o tema de Direito do Consumidor como um dos ramos em destaque na discussão, ressaltam-se os artigos da LGPD mais citados:

Tabela 9: Direito do Consumidor - Artigos mais mencionados

Temas	Decisões analisadas	% de decisões
ART. 5 II	891	23,62%
ART.42	747	19,8%
ART. 7, X	703	18,64%
ART. 44	661	17,52%

A maior parte das decisões analisadas no âmbito desta pesquisa refere-se a relações de consumo. Nesse universo, observa-se que o Poder Judiciário tem sido acionado com frequência, sobretudo em controvérsias envolvendo instituições financeiras, bancos de dados e empresas de recuperação ou proteção ao crédito, bem como de provedores de conteúdo e serviços de internet, como suscitado na seção de setores deste Relatório.

Em geral, a fundamentação das decisões articula dispositivos da LGPD com artigos do CDC, evidenciando a convergência entre os dois regimes jurídicos na solução desses litígios.

Os temas mais recorrentes acompanham, por consequência, os setores mais demandados. Por isso, sobressaem discussões relacionadas a vazamentos de dados pessoais, especialmente quando deles decorrem fraudes e golpes praticados contra consumidores, controvérsias sobre a inserção de titulares em cadastros de proteção ao crédito e em cadastros positivos, bem como na invasão de contas em redes sociais. Trata-se, portanto, de um conjunto de casos em que a proteção de dados aparece vinculada à tutela do consumidor e à discussão sobre responsabilização por danos decorrentes do uso de informações pessoais^{17 18 19}.

Como apontado anteriormente, o artigo 5º, II, da LGPD é frequentemente utilizado para distinguir os dados pessoais sensíveis dos dados pessoais comuns, bem como para estabelecer paralelos entre o conceito de dado sensível na LGPD e em normas do ordenamento jurídico. Além disso, a definição de dado pessoal sensível tem papel relevante especialmente para avaliar a possibilidade de reconhecimento de dano moral presumido, principalmente com menção expressa ao AREsp 2.130.619/SP.

-
17. Exemplificativamente: TJ-SP - Apelação Cível: 10091162720248260566 São Carlos, Relator.: Alexandre David Malfatti, Data de Julgamento: 13/12/2024, 12ª Câmara de Direito Privado, Data de Publicação: 13/12/2024. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/tj-sp/2928052603/inteiro-teor-2928052606>
 18. Exemplificativamente: TJ-MG - Apelação Cível: 50537126520228130079, Relator.: Des .(a) Amorim Siqueira, Data de Julgamento: 08/10/2024, Câmaras Cíveis / 9ª CÂMARA CÍVEL, Data de Publicação: 10/10/2024. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/tj-mg/2903369971/inteiro-teor-2903370024>
 19. Exemplificativamente: TJ-SP - Apelação Cível: 10007296820248260648 Urupês, Relator.: Rosangela Telles, Data de Julgamento: 04/02/2025, 31ª Câmara de Direito Privado, Data de Publicação: 04/02/2025. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/tj-sp/3036748386/inteiro-teor-3036748387>

Além dos setores supracitados, que foram amplamente abordados ao longo do Relatório, destaca-se também a presença de discussões sobre o tratamento de dados por operadoras de telecomunicações, bem como sua responsabilidade. Os casos costumam versar sobre a possibilidade de utilização de extratos telefônicos como meio de prova, amplamente permitida. Outro tópico frequente tem sido o de contratações realizadas fraudulentamente por terceiros, trocas indevidas de titularidade de número de chip de telefonia, bem como de bloqueio indevido de linha sem autenticação adequada perante operadoras de telefonia. Nesses casos, os tribunais têm reconhecido a responsabilidade dessas empresas quando se verifica que o alegado vazamento ou o tratamento indevido de dados pessoais do consumidor decorreu de falhas nos procedimentos internos de verificação de identidade^{20 21 22}.

Comercialização de dados pessoais. Proteção ao crédito. Cadastro positivo.

Dispositivos da LGPD citados: ART. 7º, CAPUT | ART. 7º, X | ART. 7º, § 3º | ART. 7, § 4º | ART. 8, § 3º.

Trata-se de ação condenatória em que se discute a legalidade do tratamento de dados disponibilizado por bureau de crédito, no qual as empresas possuem acesso a um relatório de análise de crédito da Pessoa Física. O autor alega que este tratamento é ilícito, excessivo e indenizável pelo dano moral consequente da comercialização indevida de suas informações pessoais, realizadas sem seu consentimento.

O Juízo destacou que o serviço está em conformidade com a LGPD, já que o serviço em questão se refere ao Cadastro Positivo, instrumento definido em lei própria, que dispensa o consentimento do indivíduo, além de que os dados constantes no relatório são extraídos de banco de dados públicos e,

-
20. Exemplificativamente: TJMG. 5001622-65.2024.8.13.0708. Juiz: Ismael Fernando Poli Villas Boas Junior. 2º Juizado Especial Cível e Criminal da Comarca de Várzea da Palma. Data de Julgamento: 09/06/2025. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/tj-mg/4146754268/inteiro-teor-4146754269>
 21. Exemplificativamente: TJSP. 0009010-83.2024.8.26.0016. Juíza: Joanna Terra Sampaio dos Santos. Juizado Especial Cível Anexo FAAP. Data de Julgamento: 21/04/2025. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/tj-sp/3508720886/inteiro-teor-3508720891>
 22. Exemplificativamente: TJMG. 5005301-84.2021.8.13.0027. Relator: Des. Habib Felipe Jabour. 18ª Câmara Cível. Data de Julgamento: 27/05/2025. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/3944750108>

são meramente cadastrais e suficientes à sua finalidade, não havendo a caracterização de comercialização de dados sensíveis.

Além disso, a decisão destaca que a própria LGPD expressamente autoriza o tratamento de dados para a finalidade de proteção ao crédito, intentando prevenir fraude e proteger os próprios cadastrados em bureau de crédito. Dessa forma, concluiu-se pelo afastamento da configuração de danos morais, uma vez que o serviço prestado pelo réu é lícito e harmoniza-se aos preceitos da LGPD.

TJSP, 10010448420248260070, Relator Juiz (a): Maria Esther Chaves Gomes, Data de Julgamento: 25/06/2025, 2º Vara Cível – Batatais, Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/4158885842>.

Invasão de perfil em rede social (hacker). Dever de segurança. Falha na prestação do serviço. Sequestro digital. Danos morais.

Dispositivos da LGPD citados: ART. 6º, VII | ART. 42 | ART. 46 | ART. 49.

Trata-se de apelação cível interposta pela rede social contra sentença que julgou parcialmente procedentes os pedidos, decorrente de ataque cibernético (hacker) na conta profissional do autor, utilizada para divulgação e comercialização de produtos, com mais de 80 mil seguidores. Após a invasão, os cibercriminosos passaram a divulgar material com cunho golpista, aplicando fraudes em nome do usuário.

O acórdão fundamentou a responsabilidade da plataforma com base na LGPD, destacando que os agentes de tratamento devem adotar medidas de segurança, nos termos do art. 46 da LGPD. Também foi suscitado o art. 49 da LGPD, que determina que os sistemas utilizados para tratamento de dados devem ser estruturados de forma a atender aos requisitos de segurança, padrões de boas práticas e de governança.

Foram ressaltados ainda o princípio da segurança (art. 6º, VII, da LGPD), e responsabilidade civil, acompanhada do dever de reparar os danos ao titular, conforme o art. 42 da LGPD. Consignou-se que as ameaças de segurança não são imprevisíveis ou inevitáveis, mas decorrem usualmente da utilização de sistemas de segurança antiquados ou fora dos padrões recomendados, de modo que a concretização de um ataque está ligada a alguma deficiência no sistema do provedor.

O dano moral foi reconhecido in re ipsa, dada a privação da conta profissional, da exposição do autor a situação vexatória perante seus seguidores e da utilização de sua credibilidade para aplicação de golpes.

A apelação foi desprovida, mantendo-se a condenação ao pagamento de indenização por danos morais.

TJ-AL - Apelação Cível: 07090986520228020001 Maceió, Relator.: Des. Orlando Rocha Filho, Data de Julgamento: 22/01/2025, 4ª Câmara Cível, Data de Publicação: 22/01/2025. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/tj-al/3005846356>

Plataforma de intermediação de transporte. Uso indevido de dados por terceiro. Bloqueio de cadastro. Vazamento de dados. Ausência de dano comprovado.

Dispositivos da LGPD citados: ART. 42

Trata-se de ação de obrigação de fazer c/c indenização por danos morais proposta por motorista parceiro contra plataforma de intermediação de transporte. O autor alegou que, ao tentar reativar seu cadastro em novembro de 2023 (inativo desde 2018), descobriu que seu CPF estava vinculado a um número de telefone de terceiro desconhecido, residente em outro estado, tendo seus dados pessoais sido utilizados indevidamente na plataforma por mais de três anos. Requereu o desbloqueio do CPF, a revinculação ao seu número de celular e indenização por danos morais.

O Juízo entendeu que o bloqueio do cadastro decorreu de exercício regular de direito pela plataforma, com base nos Termos e Condições de Uso, que vedam o compartilhamento de conta e autorizam a suspensão em caso de inconsistências cadastrais. A empresa comprovou que detectou irregularidades por meio de reconhecimento facial e que o bloqueio foi automático e preventivo, afastando má-fé ou arbitrariedade.

Quanto à LGPD, foi mencionado o art. 42 da LGPD para afirmar que a caracterização de dano em casos de vazamento ou uso indevido de dados pessoais exige a demonstração efetiva de prejuízo. No caso, embora não se tenha negado que terceiros possam ter utilizado o CPF do autor, o Juízo concluiu que não houve comprovação de que essa utilização tenha causado prejuízo concreto à esfera patrimonial ou moral do autor, entendendo que o vazamento de dados, por si só, não acarretou consequências gravosas à imagem, personalidade ou dignidade do titular.

Os pedidos foram julgados integralmente improcedentes. A sentença ressaltou, contudo, que nada impede o autor de apresentar nova solicitação de cadastro à plataforma, a ser avaliada conforme os critérios contratuais vigentes.

TJMS, 0803258-35.2024.8.12.0001, Juiz: Deni Luis Dalla Riva, 6ª Vara Cível de Campo Grande, Data de Julgamento: 19/12/2024, Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/tj-ms/3192910498/inteiro-teor-3192910509>

iii. Direito do Trabalho

Dentre as decisões que abordaram o Direito do Trabalho como um dos tópicos centrais do litígio, destacaram-se as menções dos seguintes artigos da LGPD:

Tabela 10: Direito do Trabalho - Artigos mais mencionados

Temas	Decisões analisadas	% de decisões
ART. 7, VI	278	32,4%
ART. 11, II, D	131	15,27%
ART. 6	122	14,22%
ART. 7	111	12,94%

De modo geral, as decisões fazem referência a dispositivos da LGPD relacionados às bases legais de exercício regular de direitos em processo judicial, administrativo ou arbitral, tanto de dados pessoais quanto de dados pessoais sensíveis, bem como sob a perspectiva principiológica da LGPD.

Entre os principais temas discutidos nas decisões relacionadas ao Direito do Trabalho, destacam-se: i) o fornecimento de dados de empregados a sindicatos, ii) a exibição de documentos de empregados, iii) o uso de geolocalização como prova digital em ações trabalhistas, e iv) a divulgação de dados pessoais de trabalhadores em relatórios de transparência salarial.

O fornecimento de dados de empregados a sindicatos é discutido no âmbito de convenções coletivas, com a finalidade de que os sindicatos possam fiscalizar as relações trabalhistas. Frequentemente, esses litígios abordam as bases legais de exercício regular de direitos ou para cumprimento de obrigação regulatória. Tem sido reconhecida, frequentemente, a possibilidade de concessão dos dados dos empregados aos sindicatos, embora algumas decisões afirmem tratar-se de tratamento de dados cuja base legal seria a do consenti-

mento, hipótese em que o pedido de fornecimento dos dados é julgado improcedente por ausência de autorização expressa dos empregados^{23 24}.

A discussão quanto ao uso de provas do âmbito trabalhista engloba, como tópico principal, o uso da prova de geolocalização. Tal questão é trabalhada com fundamento na base legal de exercício regular de direitos em processo judicial, administrativo ou arbitral. Em geral, há decisões que permitem a prova de geolocalização; outras afastam o seu uso, em razão da desproporcionalidade da prova e da possibilidade de as empregadoras possuírem estrutura para realizar, principalmente, o controle de jornada de outras formas^{25 26}.

Quanto aos Relatórios de transparência salarial, são postas em questão a constitucionalidade e legalidade da Lei n. 14.611/2023 e seus regulamentos (Decreto 11.795/2023 e Portaria MTE 3.714/2023). Alega-se, sob a perspectiva da LGPD, que o mero cruzamento de informações tornaria sem efeito a anonimização dos dados previstos na LGPD. Há decisões que suspendem a divulgação, mas boa parte permite que tais dados sejam divulgados, com menções à eliminação de desigualdades explícitas de remuneração entre homens e mulheres, suscitando o princípio da não discriminação da LGPD, bem como o art. 7º, II e art. 11, II, a), que permitem o tratamento de dados para fins de obrigação legal^{27 28}.

23. Exemplificativamente: TRT2: 10012722720245020604, Relator.: Ricardo Verta Ludovice, 11ª Turma. Data de Julgamento: 19/12/2024. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/trt-2/2941260157/inteiro-teor-2941260160>

24. Exemplificativamente: TRT-15. 0011780-36.2024.5.15.0071. Juiz: Luis Furian Zorzetto. Vara do Trabalho de Mogi Guaçu. Data de Julgamento: 02/12/2024. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/trt-15/2900337263/inteiro-teor-2900337264>

25. Exemplificativamente: TRT15. 0011216-60.2023.5.15.0146. Vara do Trabalho de Orlândia. Juiz. Rodrigo de Mattos Takayassu. Data de Julgamento: 25/05/2025. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/trt-15/4996173784/inteiro-teor-4996173788>

26. Exemplificativamente: TRT4. 00203811120195040007, Data de Julgamento: 05/08/2025. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/trt-4/4366275750/inteiro-teor-4366275886>

27. Exemplificativamente: TRF-3. 5001256-52.2024.4.03.6103. 2ª Vara Federal de São José dos Campos. Data de Julgamento: 14/11/2024. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/trf-3/2847828318/inteiro-teor-2847828327>

28. Exemplificativamente: TRT-4. 0020413-15.2024.5.04.0662. Redator: Ary Faria Marimon Filho. 1ª Turma. Data de Julgamento: 18/09/2025. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/trt-4/4934420760/inteiro-teor-4934420768>

Por fim, embora o art. 20 da LGPD não esteja entre os artigos mais mencionados quanto à temática trabalhista, cabe ressaltá-lo, como se abordará em tópico específico, pois tem sido tema recorrente nos tribunais e vem ganhando cada vez mais destaque frente ao uso de tecnologias. Assim, os casos tratam em geral de bloqueios e descadastramento de contas em aplicativos de intermediação de transportes, em que o empregado fica impossibilitado de exercer seus serviços, em razão da suspensão de sua conta realizada com base em decisão automatizada. Em parte das decisões, o art. 20 é articulado como fundamento para exigir que o agente de tratamento forneça informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, seguindo o decidido pelo STJ, no julgamento do Resp 2135783/DF²⁹.

Dados pessoais não sensíveis. Compartilhamento de dados com sindicato. Bases legais. Descumprimento de cláusula coletiva. Relação nominal de empregados.

Dispositivos da LGPD citados: ART. 5º, II | ART. 7º, II | ART. 7º, IX | ART. 11º, II, ALÍNEAS "A" | ART. 11, II, "D" | ART. 10, II

Trata-se de ação de cumprimento ajuizada por sindicato profissional para compelir a reclamada ao fornecimento da relação nominal de empregados, conforme previsto na cláusula 50ª da Convenção Coletiva de Trabalho. O juízo reconheceu que o descumprimento da norma coletiva autoriza a imposição de obrigação de fazer e multa normativa.

A alegação de violação à LGPD foi afastada, com a justificativa de que as informações solicitadas não configuram dados pessoais sensíveis, nos termos do art. 5º, II, da LGPD. Ademais, entendeu-se legítimo o tratamento de dados com base no art. 7º, II e IX, da LGPD, por decorrer de obrigação legal e do exercício regular de direitos, bem como no art. 11, II, d, da LGPD, conforme previsto na própria cláusula coletiva. Reconheceu-se, ainda, a atuação legítima do sindicato à luz do art. 8º, III, da Constituição Federal, mantendo-se a condenação ao cumprimento da obrigação e ao pagamento da multa da empregadora.

TRT-15, 0011928-75.2024.5.15.0094, Juíza do Trabalho Substituta Barbara Baldani Fernandes Nunes, 7ª Vara do Trabalho de Campinas, Data de Julgamento: 08/07/2025, Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/trt-15/4568592134/inteiro-teor-4568592291>

29. STJ. REsp 2135783 - DF. Relator: Ministra Nancy Andrighi. 3ª Turma. Data de Julgamento: 18/06/2024. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/stj/2939367384>

Dados pessoais comuns. Norma coletiva. Fornecimento de dados de admissão e demissão ao sindicato. Bases legais.

Dispositivos da LGPD citados: ART. 5º, I | ART. 5º, II | ART. 7º, CAPUT | ART. 7º, VI | ART. 7º, § 3º | ART. 7º, § 4º | ART. 7º, § 7º | ART. 11.

Trata-se de agravo em agravo de instrumento em recurso de revista interposto por empresa que questionava a validade de cláusula de Convenção Coletiva de Trabalho, a qual obrigava as empresas a fornecer ao sindicato profissional, em caráter confidencial, listagem de funcionários admitidos e demitidos no período de vigência da norma. A empresa alegava que a cláusula violava a LGPD, ao buscar dados sensíveis dos trabalhadores sem autorização prévia.

O TST diferenciou a caracterização de dados pessoais (art. 5º, I, e art. 7º da LGPD) e dados pessoais sensíveis (art. 5º, II, e art. 11 da LGPD). Assim, concluiu que dados como cadastrais e informações referentes à admissão e à demissão de empregados não se enquadram no conceito de dados sensíveis.

A decisão destacou que o tratamento de dados previsto na norma coletiva não viola a LGPD, uma vez que i) nos termos do art. 7º, VI, o sindicato tem o poder-dever de tutelar os direitos dos trabalhadores representados, para o exercício regular de direitos em processo judicial, administrativo ou arbitral, ii) as informações já são prestadas a sistemas públicos (e-Social), possibilitando seu compartilhamento, bem como a possibilidade de tratamento de dados para novas finalidades, nos termos do art. 7º, § 7º, da LGPD; iii) a própria cláusula prevê medidas adequadas de proteção, como confidencialidade, armazenamento seguro, eliminação dos dados em cinco anos após a rescisão contratual, e o direito do titular de apresentar repúdio à prestação de informações.

Desta forma, a Corte manteve a validade da cláusula da CCT, reconhecendo-se sua conformidade com a LGPD, por se tratar de tratamento de dados pessoais comuns, fundamentada em base legal adequada e asseguradas medidas de proteção.

TST. 0010534-26.2023.5.15.0043, Relator Min.: Alexandre Luiz Ramos, 4ª Turma, Data de Julgamento: 11/03/2025, Data de Publicação: 21/03/2025, Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/tst/3294473805/inteiro-teor-32944738> 21.

Plataforma digital de recrutamento de trabalhadores. Dano moral coletivo, Princípios da finalidade, necessidade e adequação. Questionários invasivos. Viés político e dados de saúde.

Dispositivos da LGPD citados: ART. 5, II | ART. 5, X | ART. 6º | ART. 6º, I | ART. 6º, II | ART. 6º, III | ART. 6º, IV | ART. 6º, V | ART. 6º, VI | ART. 7º | ART. 7º, I | ART. 7º, II | ART. 7º, III | ART. 7º, IV | ART. 7º, V | ART. 7º, VI | ART. 7º, VII | ART. 7º, VIII | ART. 7º, IX | ART. 7º, X | ART. 11 | ART. 37 | ART. 41 | ART. 41, §1

Trata-se de recurso ordinário em ação civil pública envolvendo tratamento de dados pessoais em processos seletivos, à luz da LGPD, julgado pelo TRT da 15ª Região. Constatou-se a coleta indevida de dados pessoais sensíveis, nos termos do art. 5º, II, bem como tratamento incompatível com o conceito legal previsto no art. 5º, X, especialmente quanto a informações de saúde e opinião política. A decisão reconheceu a violação aos princípios da finalidade, adequação, necessidade, transparência e qualidade dos dados previstos no art. 6º da LGPD. Desta maneira, manteve a decisão do Juízo originário para que a plataforma abstinhasse-se de tratar dados desnecessários e impertinentes para a finalidade informada de seleção para emprego.

Também foi ressaltado o afastamento da utilização do legítimo interesse como base válida, nos termos do art. 7º, para dados pessoais sensíveis, devendo-se o tratamento ser baseado nas hipóteses legais do art. 11 para tratamento de dados sensíveis. O Tribunal determinou que o Juízo de origem se pronunciasse a respeito de obrigações de fazer relacionadas ao art. 37 (registro das operações de tratamento) e ao art. 41 (indicação de encarregado), bem como à indicação da finalidade dos dados tratados, em cumprimento ao princípio da finalidade. Além disso, determinou-se que a sentença também se pronunciasse a respeito da necessidade de a empresa destacar em suas políticas de privacidade as bases de tratamento que utiliza para o tratamento de dados pessoais de candidatos ao emprego e de empregados, previstas no artigo 7º e/ou 11 da LGPD.

Diante da negativa de prestação jurisdicional em primeiro grau, declarou-se a nulidade parcial da decisão, determinando novo julgamento para suprir as omissões e adequar o dispositivo à fundamentação.

TRT-15. 0010333-04.2022.5.15.0032, Relator Desembargador Renan Ravel Rodrigues Fagundes, 10ª Câmara / 5ª Turma, Data de Julgamento: 11/03/2025., Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/trt-15/3243077703/inteiro-teor-3243077707>

PAINEL LGPD NOS TRIBUNAIS

4

Questões Essenciais Sobre a Aplicação da LGPD pelos Tribunais

4.1. Princípios

Os princípios previstos no art. 6º da LGPD exercem função essencial no regime jurídico de proteção de dados pessoais, operando como vetores interpretativos, critérios de conformidade normativa e parâmetros de responsabilização. Diferentemente de outros dispositivos da Lei que possuem aplicação específica, os princípios de proteção de dados estabelecem limites aplicáveis aos mais diversos contextos e deveres permanentes a serem cumpridos pelos agentes de tratamento.

Assim, a partir das decisões que fazem parte do escopo dessa pesquisa, é fundamental entender como os tribunais estão aplicando os princípios de proteção de dados, considerando que, para que um tratamento de dados esteja de acordo com a Lei, necessariamente esses princípios devem ser observados. Abaixo, relembremos todos eles:

Tabela 11: princípios da LGPD

BOA-FÉ OBJETIVA
(Art. 6º, caput)

Tratar dados seguindo ditames éticos e morais.

FINALIDADE
(Art. 6º, I)

Tratar os dados para finalidades legítimas, específicas, explícitas e informadas ao titular, abstendo-se de tratá-los posteriormente de forma incompatível com tais finalidades.

ADEQUAÇÃO
(Art. 6º, II)

Tratar os dados de forma compatível com as finalidades que foram informadas ao titular, de acordo com o contexto do tratamento.

NECESSIDADE
(Art. 6º, III)

Limitar o tratamento de dados ao mínimo necessário para a realização de suas finalidades, tratando apenas dados pertinentes, proporcionais e não excessivos em relação a tais finalidades.

LIVRE ACESSO
(Art. 6º, IV)

Viabilizar, aos titulares, a consulta facilitada e gratuita sobre (i) a forma e a duração do tratamento e (ii) a integralidade dos dados.

QUALIDADE DOS DADOS
(Art. 6º, V)

Garantir, aos titulares, a exatidão, clareza, relevância e atualização dos dados pessoais, de acordo com a necessidade e para cumprir a finalidade do tratamento.

TRANSPARÊNCIA
(Art. 6º, VI)

Garantir, aos titulares, informações claras, precisas e facilmente acessíveis sobre o tratamento e os agentes de tratamento, observados os segredos comercial e industrial.

SEGURANÇA
(Art. 6º, VII)

Utilizar medidas técnicas e administrativas aptas a proteger os dados de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.

PREVENÇÃO
(Art. 6º, VIII)

Adotar medidas para prevenir a ocorrência de danos em virtude do tratamento de dados.

NÃO DISCRIMINAÇÃO (Art. 6º, IX)

Abster-se de realizar o tratamento para fins discriminatórios ilícitos ou abusivos.

RESPONSABILIZAÇÃO E PRESTAÇÃO DE CONTAS (Art. 6º, X)

Demonstrar a adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e da eficácia de tais medidas.

Nesta edição, das decisões que fazem parte do escopo da pesquisa, ou seja, das sentenças ou acórdãos relevantes que citam artigos da LGPD, que totalizaram 5.555 decisões, 738 fazem referência expressa ao art. 6º da LGPD, que dispõe sobre princípios da proteção de dados.

Dentre os princípios mais frequentemente citados nas decisões, estão os princípios da segurança com 210 decisões, seguido do princípio da finalidade com 184 menções e o princípio da prevenção mencionado 128 vezes. Destaca-se a quantidade quase equiparada de processos que mencionam necessidade, transparência e responsabilização e prestação de contas, em torno de 100 decisões.

Quanto às menções ao art. 6º, observa-se que o caput do dispositivo aparece numericamente como o mais citado nas decisões analisadas. Embora o caput corresponda ao princípio da boa-fé, as decisões judiciais, em regra, não desenvolvem análise específica sobre esse princípio, limitando-se a mencionar genericamente a incidência dos princípios da LGPD como obrigação geral. Conclui-se que essa referência ao caput costuma servir apenas para indicar a existência de um dever amplo de conformidade com o regime principiológico da lei, sem identificação do princípio aplicável ao caso concreto ou explicitação das obrigações que dele decorreriam. Esse padrão revela uma utilização predominantemente retórica do dispositivo, o que dificulta a identificação de uma *ratio decidendi* efetiva.

Tabela 12: Artigos mais citados - Princípios

ART. 6	54,61%
ART. 6, VII	28,46%
ART. 6, I	24,93%
ART. 6, VIII	17,34%
ART. 6, III	15,18%
ART. 6, VI	13,96%
ART. 6, II	9,89%
ART. 6, IX	7,99%
ART. 6, X	5,96%
ART. 6, V	5,83%
ART. 6, IV	4,20%

Para a análise das menções aos princípios da LGPD nas decisões que compõem o espaço amostral desta pesquisa, foram considerados dois parâmetros metodológicos complementares. O primeiro refere-se às menções expressas ao art. 6º da LGPD nas decisões judiciais, critério que delimita o próprio escopo da pesquisa e permite identificar de forma objetiva quais artigos da Lei são mobilizados pelos tribunais na fundamentação das decisões. O segundo parâmetro decorre do mapeamento automatizado de termos e palavras-chave realizado com o auxílio das ferramentas de inteligência artificial do Jusbrasil, que possibilita identificar padrões discursivos nas decisões, ainda que não haja referência direta ao dispositivo correspondente da LGPD.

A combinação desses dois parâmetros permite compreender, de forma mais ampla, como determinados conceitos da proteção de dados pessoais aparecem nas decisões judiciais, seja por meio da citação direta da Lei, seja pela utilização de categorias jurídicas correlatas no contexto da fundamentação.

Tabela 13: Termos de Princípios mencionados no universo de 5.555 decisões

Segurança	1264
Finalidade	607
Transparência	547
Necessidade	395
Prevenção	385
Responsabilização e Prestação de Contas	352
Boa-Fé	338
Adequação	252
Livre Acesso	115
Não Discriminação	75

*uma mesma decisão pode mencionar múltiplos princípios da LGPD

Quanto à distribuição por instância, conforme o gráfico a seguir, observa-se que:

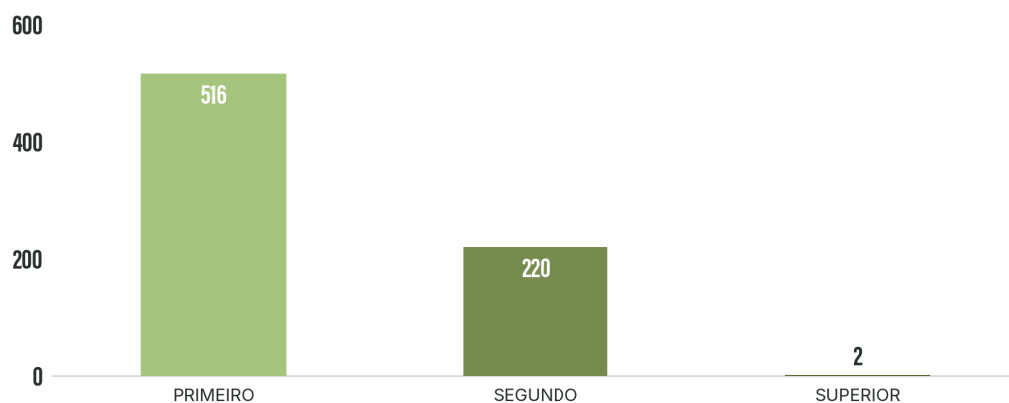


Gráfico 10: Instância mais frequente - Princípios

- 516 decisões foram proferidas em 1o grau, representando aproximadamente 70% das decisões que citam algum dos incisos ou caput do art. 6º;
- 220 em 2o grau, o que representa aproximadamente 30% das decisões;
- 2 em tribunais superiores, contabilizando somente 0,3% das decisões.

Em termos de concentração por tribunal, destaca-se a incidência mais significativa em TJs, responsáveis por em torno de 73% das decisões que mencionam expressamente princípios da LGPD.

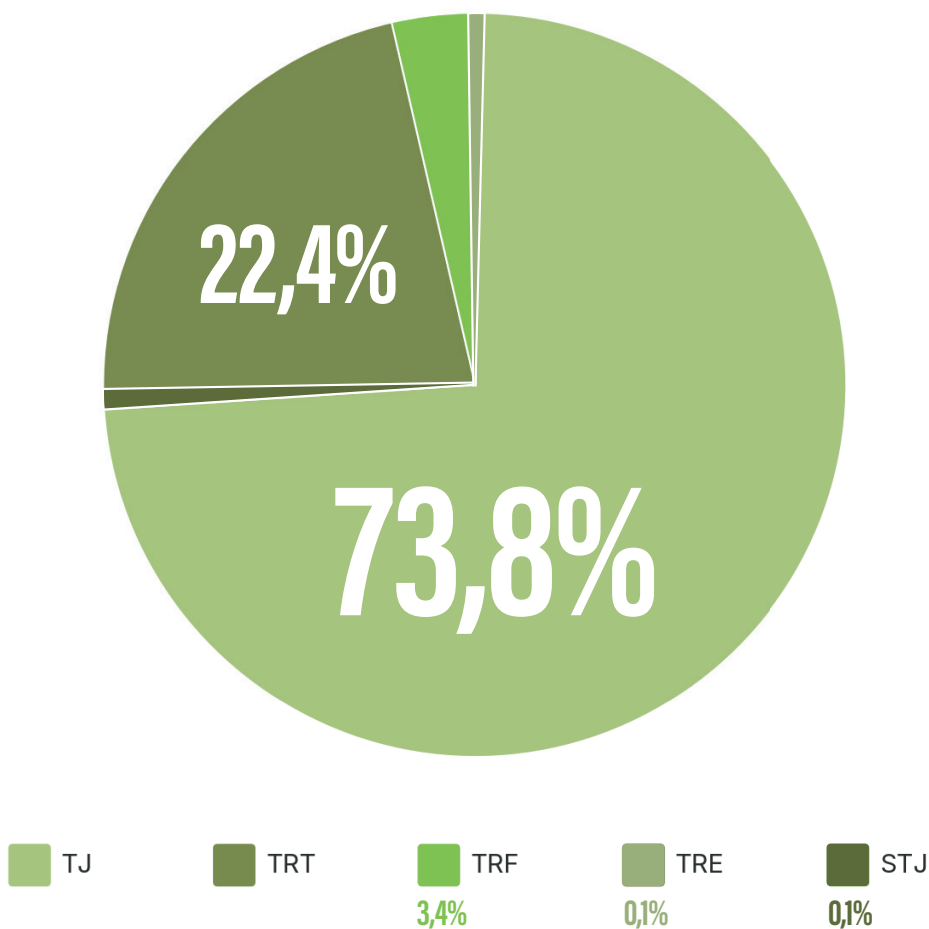


Gráfico 11: Tipo de tribunal mais frequente - Princípios

Quanto ao setor envolvido nas demandas relacionadas aos princípios, em regra, o polo ativo das decisões é composto por pessoas físicas, cerca de 88% das decisões.

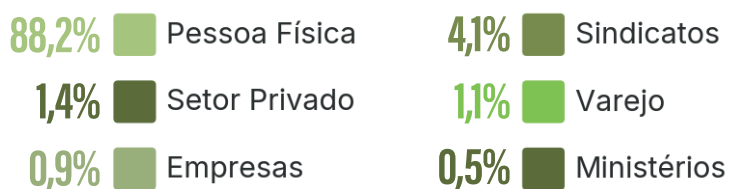
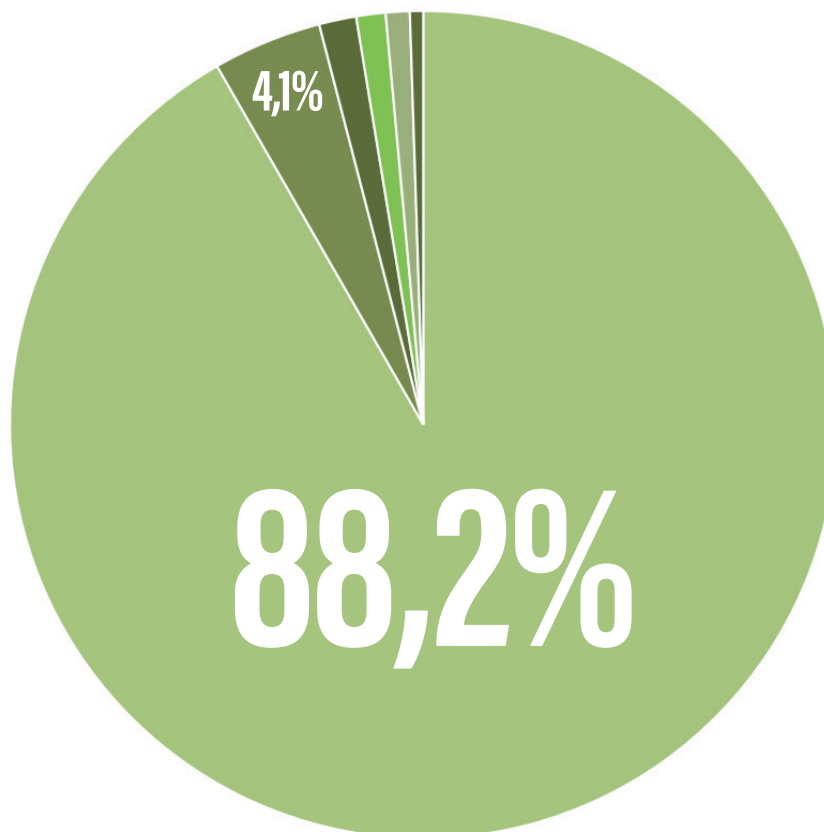


Gráfico 12: Setores mais frequentes polo ativo - Princípios

Já o polo passivo é composto por diferentes setores, sendo possível consolidar o seguinte mapeamento com os cinco setores mais frequentes:

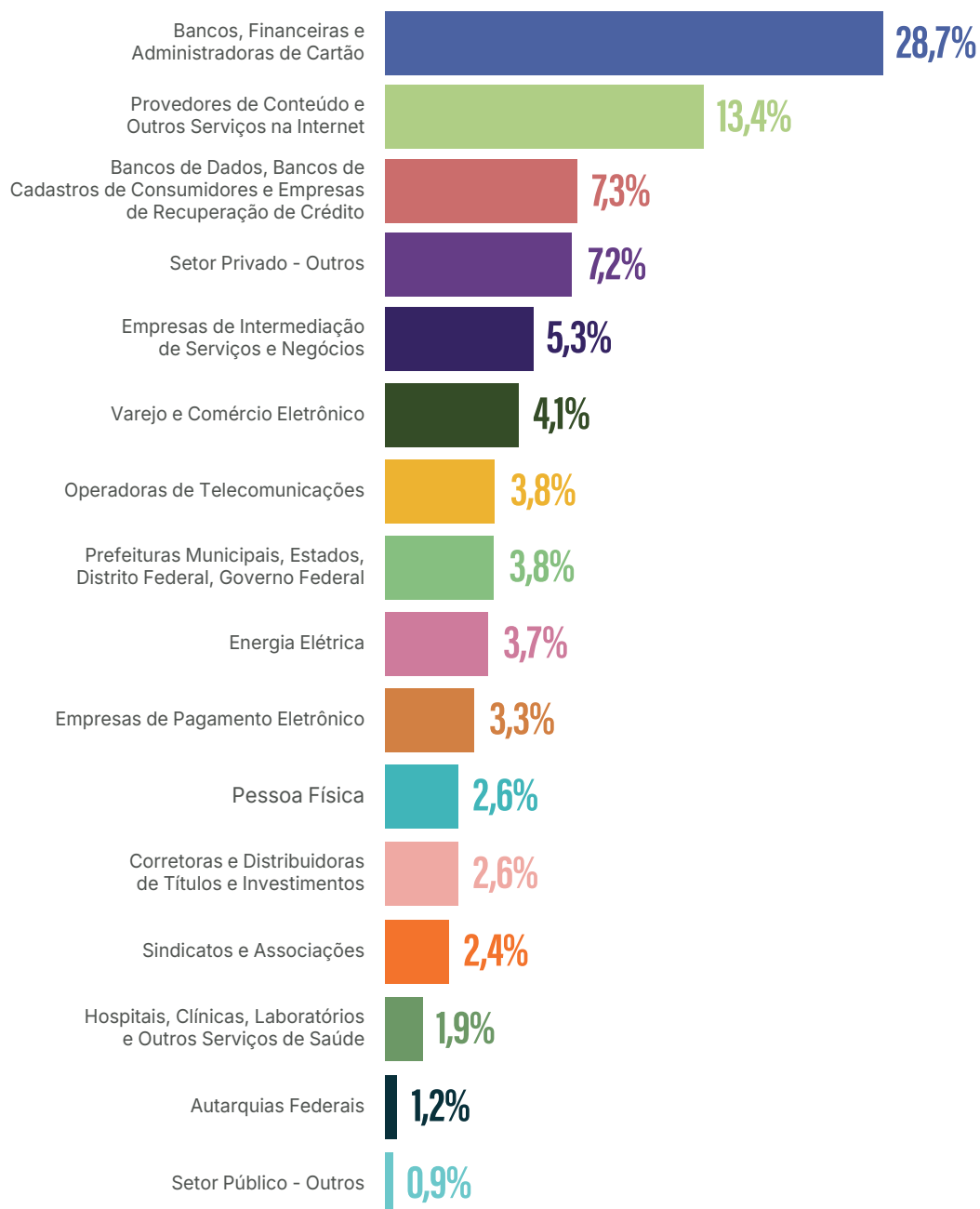


Gráfico 13: Setores mais frequentes polo passivo - Princípios

i. Princípio da Segurança (art. 6º, VII)

Assim como foi identificado na edição anterior deste Relatório³⁰, o princípio da segurança continua sendo o mais citado nas decisões judiciais que compõem o escopo da pesquisa conforme o parâmetro de artigos expressamente mais citados. A maior parte desses processos envolve situações em que os titulares alegam o comando contrário da redação do princípio: o agente de tratamento não adotou as medidas técnicas e administrativas suficientes para proteger os dados pessoais contra acessos indevidos ou contra situações de perda, destruição, alteração ou divulgação ilícita.

Em geral, grande parte dos casos analisados trata de fraudes que teriam sido possibilitadas por vazamentos de dados pessoais. Nessas ações, os titulares sustentam que o agente que detinha seus dados tinha o dever de mantê-los seguros e impedir o acesso por terceiros. A tese apresentada é a de que a falha na proteção viabiliza a fraude, estabelecendo-se, assim, o vínculo entre a violação do dever de segurança e o dano.

Também se identificam decisões em que o princípio da segurança é mencionado em situações de acesso indevido por terceiros, mesmo quando não há fraude comprovada. Nesses casos, o Judiciário reconhece que o simples fato de terceiros terem tido acesso indevido aos dados já revela possível descumprimento do dever de proteção.

Cabe ressaltar que o princípio da segurança protege os dados pessoais não somente de acessos e divulgação inadequados, mas também de utilizações indevidas, o que o torna indissociável do dever dos responsáveis de resguardar tais informações. Por isso, foram recorrentes decisões que relacionam o princípio da segurança ao regime de responsabilidade previsto no art. 42 da LGPD ao discutir a existência de dano e a obrigação de indenizar.

30. Essa conclusão também segue o entendimento da versão anterior deste Relatório: "O princípio da segurança foi o mais recorrentemente citado nos processos judiciais classificados como relevantes. Os casos que citam o princípio da segurança dizem respeito ao descumprimento da obrigação dos agentes de tratamento utilizarem 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." Disponível em: <https://static.jusbr.com/painel-igpd/edicoes/relatorio-do-painel-igpd-nos-tribunais-2025.pdf>. Acesso em 28 fev. 2026.

Outro artigo que aparece de forma recorrente nas decisões que examinam o princípio da segurança é o art. 46 da LGPD, considerado a “materialização do princípio da segurança da LGPD”.³¹ Se o art. 6º, VII, estabelece o princípio em nível axiológico ao impor a utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais, o art. 46 desloca essa diretriz para o plano da obrigação jurídica específica.

Nas decisões analisadas que mencionam o princípio da segurança, o artigo 46 costuma ser mobilizado para afastar alegações genéricas de adoção de “boas práticas” ou de cumprimento abstrato da lei, embora boa parte das decisões não aprofundem quais medidas de segurança deveriam ser adotadas. Quando violações à segurança dos dados são reconhecidas, os tribunais suscitam a ausência de demonstração concreta das salvaguardas implementadas em contextos de indícios de incidente de segurança, vazamento de dados ou acesso indevido por terceiros. Assim, o art. 46 é citado como parâmetro objetivo de aferição da diligência do agente de tratamento, sendo insuficiente afirmar que existem mecanismos de proteção, sem que estes sejam adequados ao risco da atividade desenvolvida.

ii. Princípio da Finalidade (art. 6º, I)

O princípio da finalidade exige que o tratamento de dados pessoais seja realizado para propósitos (i) legítimos, (ii) específicos, (iii) explícitos e (iv) informados ao titular, sem a possibilidade de tratamento posterior de forma incompatível com essas finalidades. De forma geral, o princípio aparece nas decisões como parâmetro central para avaliar a legitimidade do fluxo de dados ao longo do tempo. Ele impede que o tratamento se transforme em atividade aberta e indefinida, reforçando a ideia de que o uso de dados pessoais deve ser contextual, delimitado e permanentemente vinculado ao propósito que justificou sua coleta.

31. Exemplificativamente: TJMG. 5005301-84.2021.8.13.0027. Relator: Habib Felipe Jabour. 18a. Data de Julgamento: 27/05/2025. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/tj-mg/3944750108>

32. Exemplificativamente: TRT-2. 1000319-91.2025.5.02.0066. 66a Vara do Trabalho de São Paulo. Juiz: Vitor José de Rezende. Data do julgamento: 04/06/2025. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/trt-2/3977811011/inteiro-teor-3977811026>

33. Exemplificativamente: TRF3. Processo no 5004054-39.2024.4.03.6344. 8a Vara – JEF/SP. Sentença publicada em 04/06/2025. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/trf-3/3966097754/inteiro-teor-3966097759>

Embora a redação do dispositivo contenha expressões abertas como "legítimos" e "compatíveis", a sua densificação ocorre no caso concreto principalmente a partir da análise do contexto em que os dados foram coletados e das expectativas legítimas do titular. Nesse sentido, o princípio da finalidade funciona como um verdadeiro critério de razoabilidade para aferição da licitude do tratamento: ainda que exista base legal, não se admite que os dados sejam utilizados para objetivos diversos daqueles previamente informados, sob pena de desconformidade com a LGPD.

Por essa razão, os casos judiciais em que esse princípio é aplicado são variados em áreas como saúde, consumidor, trabalhista, afinal, toda e qualquer operação de tratamento de dados deve possuir uma finalidade. Assim, não há uma padronização ou recorrência estatística identificada, mas convém avaliarmos algumas tendências.

A primeira delas é o tratamento de dados pelo setor público. Em geral, esse conjunto de decisões cita o princípio da finalidade associado aos princípios da adequação (art. 6º, II) e necessidade (art. 6º III), em um trinômio de argumentação.

Além disso, a esfera trabalhista aparece com grande variedade de tribunais citando o princípio da finalidade na fundamentação em casos que variam desde as "listas sujas" de empregados (inclusive com menções ao princípio da não discriminação, art. 6º, IX) até a anonimização de dados em processos judiciais trabalhistas.

Outra tendência relevante identificada diz respeito às demandas em que a ocorrência de fraude é atribuída a falhas no tratamento de dados pessoais. Nessas hipóteses, o princípio da finalidade é frequentemente mencionado em associação ao da segurança, para sustentar que o controlador não apenas deve definir finalidades legítimas e informadas, mas também estruturar o tratamento de modo a impedir que os dados escapem desse escopo.

A argumentação desenvolvida nas decisões parte da seguinte premissa: se os dados foram coletados para determinada finalidade contratual ou administrativa, sua utilização por terceiros para prática de fraude revela uma ruptura na cadeia legítima de tratamento. Ainda que o ato fraudulento seja cometido por terceiro, examina-se se o agente de tratamento permitiu, por ação ou omissão, que as informações fossem acessadas e utilizadas para objetivos completamente dissociados daqueles comunicados ao titular. Nessa perspectiva, a fraude

não é analisada apenas como falha de segurança, mas como indício de desvio da finalidade originalmente estabelecida.

iii. Princípio da Prevenção (art. 6º, VIII)

O terceiro princípio mais mencionado no espaço amostral analisado foi o da prevenção (art. 6º, VIII). O núcleo axiológico do princípio já vinha orientando a prática decisória nos tribunais; contudo, observou-se nesta edição a sua citação expressa de forma mais frequente em comparação aos demais princípios que o seguem, o que evidencia a sua importância crescente no contexto da responsabilização por falhas na proteção de dados.

A prevenção na LGPD estabelece que os agentes de tratamento devem adotar medidas destinadas a prevenir a ocorrência de danos aos titulares decorrentes de um tratamento inadequado dos dados pessoais. Em termos práticos, esse princípio impõe aos agentes o dever de estruturar seus processos e sistemas de modo a antecipar, evitar e mitigar ao máximo os riscos de prejuízos aos titulares.

Nesse sentido, a análise das decisões mostra que praticamente todas as decisões que mencionam o princípio da prevenção o fazem em conjunto com o princípio da segurança (art. 6º, VII), principalmente em casos envolvendo fraudes digitais, invasão de contas e transações bancárias fraudulentas. Nessas situações, os tribunais costumam afirmar que os agentes de tratamento, como instituições financeiras e plataformas digitais, têm o dever de adotar medidas

34. Exemplificativamente: TJPE. 0019143-19.2024.8.17.2480. Câmara Regional de Caruaru – 2a Turma. Relator Des. Paulo Augusto de Freitas Oliveira. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/tj-pe/3357500465/inteiro-teor-3357500468>

35. Exemplificativamente: TRT9. 0001437-39.2024.5.09.0041. 21a Vara do Trabalho de Curitiba. Sentença proferida em 09/07/2025. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/trt-9/5458205006/inteiro-teor-5458205008>

36. Exemplificativamente: TRT-7. 60.2024.5.07.0034. 2a Turma. Relator: Des. João Carlos de Oliveira Uchoa. Julgado em 03/02/2025. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/trt-7/3038165136/inteiro-teor-3038165138>

37. Exemplificativamente: TJMA. 0801814-82.2024.8.10.0013. 8o Juizado Especial Cível e das Relações de Consumo de São Luís. Juíza: Suely Oliveira Santos Feitosa. Sentença proferida em 30/04/2025. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/tj-ma/3819728738/inteiro-teor-3819728744>

técnicas e administrativas aptas a proteger os dados pessoais contra acessos não autorizados e vazamentos de informações.

Em diversos casos, o princípio da prevenção aparece como um dos fundamentos para caracterizar falha na prestação do serviço, quando se verifica que os mecanismos de segurança adotados pelo fornecedor não foram suficientes para evitar a ocorrência de fraude.

Em litígios envolvendo golpes bancários ou movimentações atípicas em contas digitais, algumas decisões destacam que cabe às instituições financeiras estruturar seus sistemas de forma a identificar operações suspeitas e impedir a consumação do dano, sobretudo quando se trata de transações incompatíveis com o padrão de uso do consumidor.

De modo semelhante, em casos de invasão de contas em redes sociais, os julgados apontam que os provedores de aplicação, na condição de agentes de tratamento de dados, devem implementar mecanismos capazes de evitar acessos indevidos e alterações não autorizadas em perfis de usuários, sob pena de responsabilização pelos danos decorrentes da violação de dados pessoais.

Assim, entende-se que a essência do princípio da prevenção funciona, em geral, como direcionamento para avaliar o padrão de diligência esperado do agente de tratamento quando o risco decorre da própria atividade econômica explorada. Essa lógica aproxima o princípio da prevenção das obrigações de governança e gestão de riscos previstas na própria LGPD no que se refere à adoção de medidas técnicas e administrativas voltadas à proteção de dados pessoais.

Esses entendimentos das decisões indicam que, na prática jurisprudencial, o princípio da prevenção tem sido interpretado como uma dimensão anteci-

38. Exemplificativamente: TJDFT. 0721448-19.2024.8.07.0020. 2o Juizado Especial Cível de Águas Claras. Juíza: Andreza Alves de Souza. Sentença proferida em 25/02/2025. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/tj-df/3092550106/inteiro-teor-3092550113>

39. Exemplificativamente: TJDFT. 0717909-87.2024.8.07.0006. 2o Juizado Especial Cível e Criminal de Sobradinho. Juíza: Keila Cristina de Lima Alencar Ribeiro. Sentença publicada em 05/03/2025. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/tj-df/3129690217/inteiro-teor-3129690224>

40. Exemplificativamente: TRT-7. 60.2024.5.07.0034. 2a Turma. Relator: Des. João Carlos de Oliveira Uchoa. Julgado em 03/02/2025. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/trt-7/3038165136/inteiro-teor-3038165138>

patória do dever de segurança no tratamento de dados pessoais, funcionando como parâmetro para avaliar se o agente de tratamento adotou medidas suficientes para evitar a ocorrência do dano. Contudo, a sua aplicação ainda ocorre quase sempre associada a outros fundamentos normativos da LGPD, em especial com o princípio da segurança e o regime de responsabilidade civil, não sendo identificadas decisões com construções de uma fundamentação autônoma baseada exclusivamente na prevenção.

iv. Princípio da Transparência (art. 6º, VI)

O princípio da transparência (art. 6º, VI, da LGPD) destacou-se quando observado o segundo parâmetro metodológico do tópico de princípios, baseado no mapeamento automatizado de termos e palavras-chave pela ferramenta de inteligência artificial do Jusbrasil. Esse critério permitiu identificar menções ao conceito de “transparência” nas decisões judiciais mesmo sem referência expressa ao dispositivo da LGPD.

Em muitos casos, o termo aparece associado ao dever de informação previsto no Código de Defesa do Consumidor (CDC), sendo utilizado em sentido mais amplo nas relações de consumo, demonstrando que a menção à transparência nem sempre corresponde à aplicação direta do princípio previsto na LGPD.

Como o espaço amostral da pesquisa considera apenas decisões com menção expressa a dispositivos da LGPD, essas ocorrências não foram contabilizadas como aplicação direta do art. 6º, VI. Ainda assim, a recorrência do termo revela um diálogo frequente entre proteção de dados pessoais e direito do consumidor nas decisões judiciais.

Nesse contexto, as decisões analisadas revelam uma crescente preocupação do Judiciário com a dimensão informacional da proteção de dados quanto ao dever de clareza na comunicação com o titular.

O princípio da transparência exige a garantia do fornecimento, por parte dos agentes de tratamento, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes, observados o segredo comercial e industrial, devendo ser observado não somente quando os dados são coletados, mas durante todo o ciclo de vida.

Nas decisões examinadas, a transparência aparece de forma reiterada nas controvérsias envolvendo suspensão, bloqueio ou desativação de contas em plataformas de redes sociais principalmente quando a medida é fundamentada apenas em referência genérica à “violação das diretrizes da comunidade” ou aos “termos de uso” da plataforma.

Nesses casos, os tribunais têm aplicado de maneira articulada o art. 6º, I (finalidade), o art. 6º, VI (transparência) e o art. 2º, II (autodeterminação informativa) da LGPD, entendendo que a gestão de perfis e a imposição de restrições constituem formas de tratamento de dados pessoais que devem observar critérios claros, específicos e previamente informados ao usuário. A ausência de indicação concreta da conduta supostamente irregular, somada à inexistência de oportunidade de manifestação prévia, tem sido interpretada como violação ao dever de informação qualificada e à boa-fé objetiva, configurando falha na prestação do serviço.

Observa-se, ainda, que o princípio da transparência é frequentemente articulado com o direito de acesso previsto no art. 18 da LGPD. Em diversos julgados, o descumprimento do dever de prestar informações claras e completas sobre os dados tratados é analisado não apenas sob a ótica principiológica, mas também como violação concreta a direitos do titular em contextos de recusa injustificada ou resposta incompleta a solicitações formais, até mesmo sem a menção explícita ao art. 18 da LGPD, como pode ser visualizado no caso a seguir.

41. Exemplificativamente: TJSP. 1024779-89.2023.8.26.0068. 14a Câmara de Direito Privado. Relator: Des. Penna Machado. Julgado em 08/10/2024. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/tj-sp/2779432926/inteiro-teor-2779432973>

42. Exemplificativamente: TJSP. 1068224-27.2024.8.26.0100. 44a Vara Cível da Comarca de São Paulo. Julgado em 24/01/2025. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/tj-sp/3144771244/inteiro-teor-3144771258>

Falha de segurança em portabilidade de linha ("Sim Swap"). Fraude. Responsabilidade objetiva. Segurança.

Dispositivos da LGPD citados: ART. 60, VII | ART. 42, CAPUT.

Trata-se de ação de indenização por danos morais ajuizada por consumidora em face de operadora de telefonia, em razão da troca indevida de chip ("golpe sim swap"), que permitiu a terceiro assumir o controle da linha telefônica e acessar aplicações bancárias vinculadas ao número, realizando transferências e operações fraudulentas.

A autora sustentou falha na prestação do serviço quanto à ausência de mecanismos eficazes de verificação de identidade, o que teria viabilizado o acesso indevido a seus dados pessoais e financeiros.

No julgamento das apelações, o Tribunal reconheceu a responsabilidade objetiva da operadora, afastando a alegação de culpa exclusiva de terceiro. O acórdão destacou que a fraude, embora praticada por terceiro, decorre de fortuito interno, ligado ao risco da própria atividade econômica desenvolvida pela fornecedora. Nesse contexto, a decisão articulou o regime do art. 14 do CDC com o princípio da segurança previsto no art. 6o, VII, da LGPD, enfatizando que o tratamento de dados pessoais deve observar medidas técnicas e administrativas aptas a impedir acessos não autorizados.

A Corte consignou que não houve demonstração, pela operadora, da adoção de protocolos rígidos de checagem de identidade capazes de evitar a troca indevida do chip. Assim, entendeu caracterizada a falha no dever de segurança e, conseqüentemente, o dever de indenizar, nos termos do art. 42, caput, da LGPD, que impõe a reparação quando o tratamento de dados pessoais, em violação à legislação, causar dano patrimonial ou moral.

Os dados envolvidos eram dados pessoais vinculados à linha telefônica e dados financeiros acessados a partir da fraude. O Tribunal concluiu que a indevida portabilidade da linha e o subsequente acesso a informações bancárias extrapolam o mero aborrecimento cotidiano, atingindo a esfera da personalidade da consumidora, com violação à privacidade e à segurança patrimonial. Ao final, negou provimento a ambos os recursos, mantendo a condenação da operadora ao pagamento de indenização por danos morais no valor fixado na sentença.

TJMG. 5005301-84.2021.8.13.0027. Relator: Habib Felipe Jabour. 18a Câmara Cível. Data de Julgamento: 27/05/2025. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/tj-mg/3944750108>

Falha de segurança. Acesso indevido. Responsabilidade objetiva da União e instituição financeira.

Dispositivos da LGPD citados: ART. 60, VII | ART. 42, CAPUT | ART. 42, §10, I | ART. 42, §10, II | ART. 42, §20 | ART. 42, §30 | ART. 42, §40 | ART. 43, CAPUT | ART. 43, I | ART. 43, II | ART. 43, III | ART. 44, CAPUT | ART. 44, I | ART. 44, PARÁGRAFO ÚNICO | ART. 45 | ART. 46.

Trata-se de ação em que o autor pleiteou o ressarcimento de valores relativos à restituição do Imposto de Renda de Pessoa Física, que foram desviados após alteração fraudulenta de seus dados bancários na plataforma gov.br, bem como indenização por danos morais. Constatou-se que terceiros acessaram indevidamente a conta gov.br do autor, modificaram os dados bancários cadastrados na Receita Federal e viabilizaram a abertura de contas em instituições financeiras para recebimento da restituição.

O Juízo reconheceu, preliminarmente, a legitimidade passiva da União, destacando que lhe compete a gestão e proteção dos dados pessoais inseridos em seus bancos de dados, inclusive na plataforma gov.br.

Foi invocado o art. 6o, VII, que consagra o princípio da segurança, impondo a adoção de medidas técnicas e administrativas aptas a proteger os dados pessoais contra acessos não autorizados. O Juízo ressaltou que, tratando-se de sistema informatizado gerenciado pelo Estado e destinado ao tratamento massivo de dados pessoais, inclusive financeiros e tributários, incide o dever reforçado de proteção.

Além disso, houve aplicação direta do regime de responsabilidade civil previsto nos arts. 42 a 46 da LGPD. O art. 42 foi citado como fundamento normativo para o dever de reparação quando o controlador ou operador, no exercício de atividade de tratamento, causar dano em violação à legislação de proteção de dados. O art. 43 foi referido quanto às hipóteses de exclusão de responsabilidade (inexistência de tratamento, ausência de violação ou culpa exclusiva do titular ou de terceiro) que não foram demonstradas no caso concreto.

O art. 44 foi utilizado como critério de aferição da irregularidade do tratamento no que concerne à expectativa legítima de segurança que o titular pode razoavelmente esperar do sistema. Já o parágrafo único desse dispositivo foi articulado com o art. 46, para afirmar que responde pelos danos o controlador que deixa de adotar as medidas de segurança adequadas. O Juízo concluiu que houve falha na proteção dos dados do autor na plataforma gov.br, caracterizando tratamento irregular por ausência de salvaguardas eficazes contra alteração indevida de dados bancários.

TRF3. 5004054-39.2024.4.03.6344. 8a Vara – JEF/SP. Juiz: Anderson Fernandes Vieira. Publicado em 04/06/2025. Disponível em: https://www.jus-brasil.com.br/jurisprudencia/trf-3/3966097754/inteiro-teor-3966_097759

Acesso a prontuário médico. Dados de Saúde. Direito de Acesso. Princípios da LGPD.

Dispositivos da LGPD citados: ART. 6O, I | ART. 6O, II | ART. 6O, III | ART. 18.

Trata-se de Remessa Necessária em Mandado de Segurança impetrado por paciente idosa em face de autoridade vinculada à Unidade de Pronto Atendimento (UPA 24h) de Caruaru/PE, diante da negativa de fornecimento de cópia integral de seu prontuário médico. A sentença de primeiro grau concedeu a segurança, determinando o acesso integral à documentação clínica, com fundamento na Constituição Federal, na LGPD e em normas do Conselho Federal de Medicina.

Submetida ao reexame obrigatório, a controvérsia concentrou-se na verificação da existência de direito líquido e certo ao acesso aos próprios dados de saúde e na legalidade da conduta administrativa que dificultou ou negou tal acesso. O acórdão destacou que o prontuário médico contém dados pessoais sensíveis, nos termos do art. 5o, II, da LGPD, e que a Lei assegura ao titular o direito de acesso facilitado às informações relativas ao tratamento de seus dados (art. 18). Nesse contexto, o direito do paciente não se restringe a uma faculdade administrativa, mas constitui prerrogativa legal expressa quando o documento é necessário à continuidade do tratamento em outra unidade de saúde.

A decisão também articulou os princípios do art. 6o da LGPD (finalidade, adequação e necessidade) à luz da interpretação conferida pelo Supremo Tribunal Federal no julgamento da ADI 6.649 e da ADPF 695. O Tribunal ressaltou que o tratamento de dados pessoais pelo Poder Público deve observar propósitos legítimos, específicos e explícitos (art. 6o, I), manter compatibilidade com as finalidades informadas (art. 6o, II) e limitar-se ao mínimo necessário (art. 6o, III).

No caso concreto, a negativa de acesso ao prontuário foi considerada incompatível com a própria finalidade do tratamento dos dados de saúde, que é, primordialmente, a prestação adequada de assistência médica. Impedir que a titular tenha acesso às suas informações clínicas inviabiliza a continuidade do cuidado e desvirtua o propósito legítimo que justifica a coleta e manutenção desses dados pelo ente público.

O acórdão enfatizou que a máxima proteção dos dados pessoais sob custódia estatal não se confunde com restrição ao titular, mas, ao contrário, implica assegurar-lhe controle e acesso às informações que lhe dizem respeito. Assim, a conduta administrativa foi qualificada como ilegal, por violar o direito de acesso previsto na LGPD e princípios constitucionais como a dignidade da pessoa humana e o direito à saúde.

TJPE. 0019143-19.2024.8.17.2480. Câmara Regional de Caruaru – 2a Turma. Relator Des. Paulo Augusto de Freitas Oliveira. Publicado em: 02/04/2025. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/tj-pe/3357500465/inteiro-teor-3357500468>

Exibição de contratos bancários. Direito de acesso do titular. Princípio da transparência

Dispositivos da LGPD citados: ART. 6º, VI | ART. 18, II

Trata-se de Apelação Cível interposta por instituição financeira contra sentença que julgou procedente ação de produção antecipada de provas, voltada à exibição de contratos de empréstimo consignado, portabilidade, comprovantes de TED, autorizações de desconto em folha, contratos de financiamento e seguro prestamista.

O autor alegou que firmou contratos com o banco e que, diante da ausência de acesso à documentação, encaminhou notificação extrajudicial por e-mail, sem resposta. A sentença reconheceu o direito à exibição dos documentos.

O acórdão consignou que o pedido de exibição estava fundado, entre outros fundamentos, no princípio do livre acesso previsto na Lei no 13.709/2018 (art. 6º, VI), bem como no direito de informação assegurado ao consumidor (art. 6º, III, do CDC). Destacou-se que, nos termos do art. 18, II, da LGPD, o titular tem direito de obter do controlador, a qualquer momento e mediante requisição, acesso aos seus dados.

TJSP. 1024779-89.2023.8.26.0068. 14a Câmara de Direito Privado. Relator Des. Penna Machado. Julgado em 08/10/2024. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/2779432926>

4.2. Bases legais

As bases legais são as hipóteses que legitimam as atividades de tratamento de dados pessoais, descritas na LGPD em seus artigos 7º e 11º. Trata-se de requisito de legitimação aplicável a todas as atividades de tratamento de dados pessoais, de modo a ser um tópico comumente tratado em decisões judiciais acerca da legislação.

Tabela 14: Bases legais

BASES LEGAIS (ART. 7º)	BASES LEGAIS - DADOS SENSÍVEIS (ART. 11)
Consentimento (inciso I)	Consentimento, específico, destacado, para finalidades específicas (inciso I)
Cumprimento de obrigação legal (inciso II)	Cumprimento de obrigação legal (inciso, II, a)
Execução de políticas públicas, pela administração pública (inciso III)	Execução de políticas públicas, pela administração pública (inciso II, b)

BASES LEGAIS (ART. 7º)

Realização de estudos por órgão de pesquisa (inciso IV)

Execução de contrato (inciso V)

Exercício regular de direitos (inciso VI)

Proteção da vida ou incolumidade física do titular ou de terceiros (inciso VII)

Tutela da saúde (inciso VIII)

Legítimo interesse (inciso IX)

Proteção do crédito (inciso X)

BASES LEGAIS - DADOS SENSÍVEIS (ART. 11)

Realização de estudos por órgão de pesquisa (inciso II, c)

Exercício regular de direitos, inclusive em contrato (inciso II, d)

Proteção da vida ou incolumidade física do titular ou de terceiros (inciso II, e)

Tutela da saúde (inciso II, f)

Garantia da prevenção à fraude e à segurança do titular (inciso II, g)

Assim como na seção de princípios, para a análise das menções às bases legais da LGPD nas decisões que compõem o espaço amostral desta pesquisa, foram considerados dois parâmetros metodológicos complementares. O primeiro refere-se às menções expressas aos artigos da LGPD nas decisões judiciais que indicam as bases legais, bem como artigos relacionados à aplicação das bases legais, critério que delimita o próprio escopo da pesquisa e permite identificar de forma objetiva quais artigos da Lei são mobilizados pelos tribunais na fundamentação das decisões. O segundo parâmetro decorre do mapeamento automatizado de termos e palavras-chave realizado com o auxílio das ferramentas de inteligência artificial do Jusbrasil, que possibilita identificar padrões discursivos nas decisões, ainda que não haja referência direta ao dispositivo correspondente da LGPD.

A combinação desses dois parâmetros permite compreender, de forma mais ampla, como determinados conceitos da proteção de dados pessoais aparecem nas decisões judiciais, seja por meio da citação direta da Lei, seja pela utilização de categorias jurídicas correlatas no contexto da fundamentação.

As menções ao art. 7º e 11 ocorreram em 2.351 decisões⁴³. Nota-se a prevalência de menção aos incisos e caput do art. 7º, o que ocorreu em 2.188 das decisões de todo o escopo da pesquisa (ou seja, das 5.555 decisões). O art. 11, por sua vez, foi mencionado em 567 decisões.

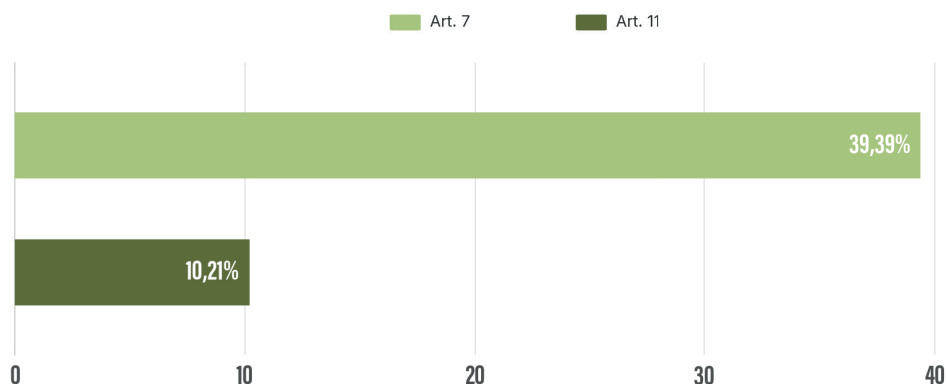


Gráfico 14: Decisões com menção aos artigos de bases legais da LGPD
(% de decisões em relação ao total de decisões do escopo da pesquisa)

43. O total de 2.351 decisões refere-se a decisões que podem ter citado os artigos 7º e 11 cumulativamente ou separadamente em uma mesma decisão.

Em números totais, entre as 5.555 decisões, 2.584 contam com menção à base legal em seu corpo, seja a partir de menções i) a bases legais específicas de forma explícita na decisão⁴⁴, seja pela menção ii) ao tema das bases legais, sem necessariamente haver menção ao artigo da LGPD correspondente à hipótese legal mencionada,⁴⁵ seja pela menção explícita das bases legais dos arts. 7º e 11, da LGPD. Em termos de decisões que incluíam menções de palavras que remeteram às bases legais,⁴⁶ nota-se uma preponderância de menção ao consentimento, vide abaixo:

Tabela 15: Termos de Bases legais mencionados no universo de 5.555 decisões

Consentimento	857
Proteção ao crédito	809
Exercício regular de direitos	805
Cumprimento de obrigação legal ou regulatória	234
Legítimo interesse	208
Prevenção à fraude e segurança	171
Execução de contrato	139
Execução de políticas públicas	98
Tutela da saúde	29
Proteção da vida ou integridade física	27
Realização de estudos por órgão de pesquisa	23

44. Exemplificativamente: TJSP. 10044313620248260417, Juiz Mariana Moraes Labre, data de julgamento 03/09/2025. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/tj-sp/5395683116/inteiro-teor-5395683117>. TJMG. 50000789420248130335, data de julgamento 27/05/2025. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/3932725436>.

45. Exemplificativamente: TJPR. 6808420238160057, Des. Rel. Dartagnan Serpa Sa, data de julgamento 26/09/2025. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/5002182818>. TRT-9. 6807720245090095, Des. Rel. Edmilson Antonio de Lima, data de julgamento 02/07/2025. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/trt-9/5454246046>.

46. Para o mapeamento colacionado abaixo quanto aos termos relacionados às bases legais, foram consideradas apenas menções às bases legais da LGPD quando mencionadas expressamente ou quando houve discussão substantiva sobre sua aplicação, ainda que sem referência ao dispositivo específico correspondente, desde que relevante para a fundamentação ou para o resultado da decisão.

Essas menções, por sua vez, não necessariamente envolvem citação dos artigos e incisos referentes às bases legais. No caso do consentimento, por exemplo, os arts. 7º, I, 8º e 11, I, referentes ao consentimento, foram citados 379, 218 e 72 vezes, respectivamente. Verificou-se que o consentimento foi discutido sem menção a tais dispositivos em ao menos 220 decisões⁴⁷.

Entre as 5.555 decisões, 2.450 mencionam artigos relacionados a bases legais⁴⁸ - quais sejam, os arts. 7º, 8º, 10, 11, 14 e 26. Assim, nesta edição do Relatório, os arts. 8º, 10, 14 e 26 foram considerados para a seleção de um universo de decisões que mencionassem dispositivos relacionados a bases legais.⁴⁹ Optou-se por essa inclusão, uma vez que é possível que haja debate acerca dos critérios para aplicação das bases legais de consentimento, legítimo interesse e execução de políticas públicas a partir da menção desses dispositivos.⁵⁰

Com relação ao art. 8º, observa-se que existe um conjunto de ao menos 65 decisões que se apoiam no dispositivo para discutir os requisitos do consentimento, sem referir-se aos arts. 7º e 11. Igualmente, com relação ao art. 10º, foram identificadas 39 decisões que o mencionaram sem fazer referência ao art. 7º, IX.

Já com relação ao art. 26, referente ao tratamento de dados pessoais pelo Poder Público, nota-se que há poucas menções a ele sem que esteja vinculado a outros artigos.

47. Exemplificativamente: TJSP. 10003993320248260596, Des. Rel. Ferreira da Cruz, DJe 27.02.2025. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/3100643395>; TJPA. 8058966220218140301, DJe 09/03/2025. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/tj-pa/5110455898/inteiro-teor-5110455909>.

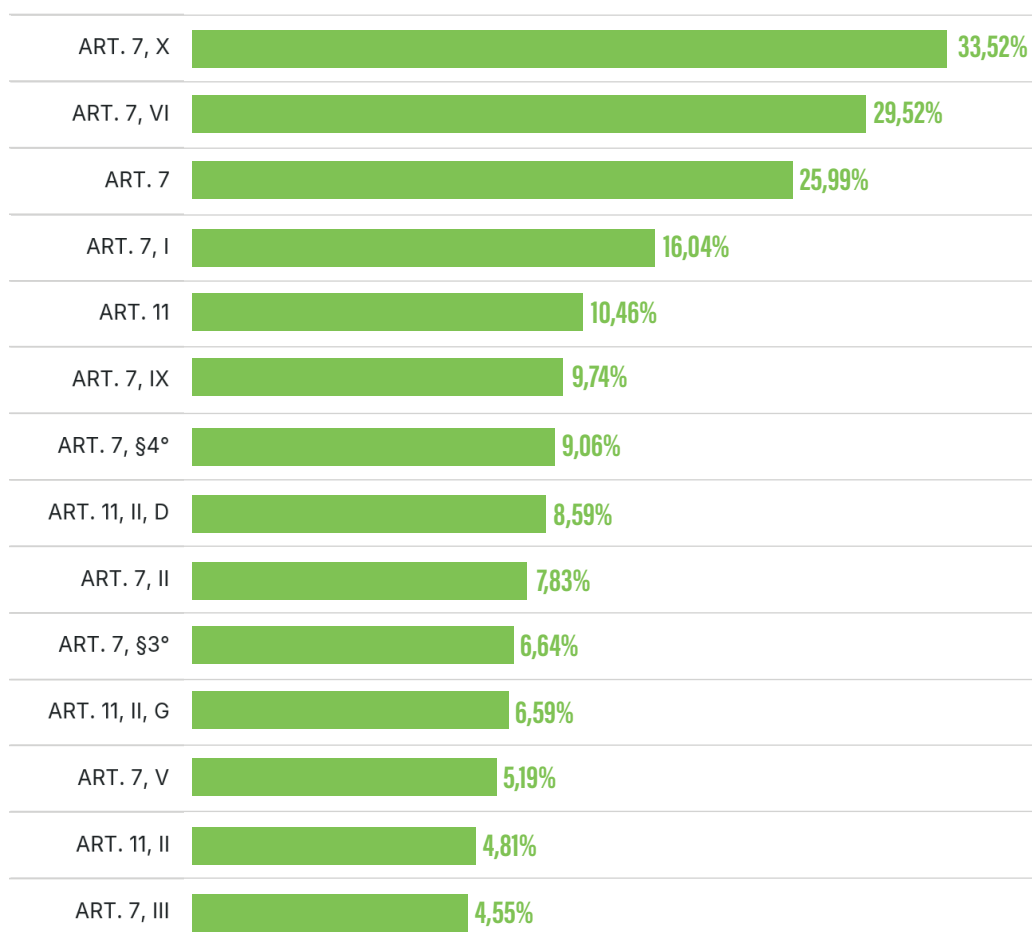
48. Ou seja, não se trata de artigo que necessariamente corresponde à base legal em si (arts. 7º e 11), mas também àquele que de alguma maneira se refere à base legal e à forma de aplicação da base legal.

49. Na terceira edição (2023), os arts. 8º e 10 também foram incluídos, enquanto nenhum dos dispositivos mencionados foi utilizado como critério na quarta edição (2024). Destaca-se que não se entende que esses artigos representam bases legais autônomas. Com efeito, a baixa incidência de decisões relevantes que mencionam esses artigos sem referência aos seus correspondentes nos arts. 7º e 11 aponta para essa conclusão, como é descrito abaixo.























50. Exemplificativamente, nos dois casos a seguir, são discutidos critérios de validade de consentimento, sem menção ao art. 7º: TJSP, 1113271-58.2023.8.26.0100, Juíza Rel. Tamara Hochgreb Matos, data de julgamento 29/05/2025, disponível em: <https://www.jusbrasil.com.br/jurisprudencia/3936747751>; TRF-4, 5010408-63.2022.4.04.7107, data de julgamento 27/11/2024, Des. Rel. Luís Alberto D'Azevedo Aurvalle, disponível em: <https://www.jusbrasil.com.br/jurisprudencia/3651896534>.

Com relação ao art. 14, por sua vez, que aborda o tratamento de dados pessoais de menores de idade, observou-se sua menção em tão somente 5 decisões, com mais da metade delas tratando do direito de imagem. Com a entrada em vigor da Lei no 15.211/2025 em março de 2026, será interessante observar as tendências sobre o tema, considerando que a norma introduz regras sobre o tratamento de dados pessoais de crianças e adolescentes. Conforme tendência já mapeada em edições anteriores, os dispositivos referentes à base legal possuem destaque entre os artigos mais citados. Como mencionado na seção 3.a., dos 20 artigos mais citados, 9 artigos referem-se às hipóteses legais, com prevalência de menções ao art. 7º, em comparação ao art. 11. Em termos de percentuais de menções a artigos, observa-se uma continuidade com relação aos Relatórios anteriores, com a preponderância dos debates sobre o art. 7º, X, relativo à base legal de proteção de crédito.

Tabela 16: Artigos mais mencionados - Bases legais



RELATÓRIO DO PAINEL NOS TRIBUNAIS

ART. 11, II, A		3,19%
ART. 11, I		3,06%
ART. 7, VII		2,34%
ART. 7, IV		2,30%
ART. 7, §7º		2,04%
ART. 7, VIII		1,91%
ART. 11, II, B		1,23%
ART. 11, II, E		1,19%
ART. 7, §5º		1,11%
ART. 11, II, C		0,94%
ART. 11, II, F		0,94%
ART. 7, §6º		0,89%
ART. 11, §2º		0,55%
ART. 11, §3º		0,34%
ART. 11, §1º		0,34%
ART. 11, §4º		0,34%
ART. 7, §1º		0,30%
ART. 7, §2º		0,26%
ART. 11, §5º		0,21%
ART. 11, §4º, II		0,21%
ART. 7, §3º, X		0,21%
ART. 11, §4º, I		0,17%

Os gráficos a seguir indicam a porcentagem das bases legais dos arts. 7º e 11 mais citados no âmbito das decisões que mencionam, respectivamente, os arts. 7º e 11:

Tabelas 17: Incisos e caput do art. 7º mencionados (%)

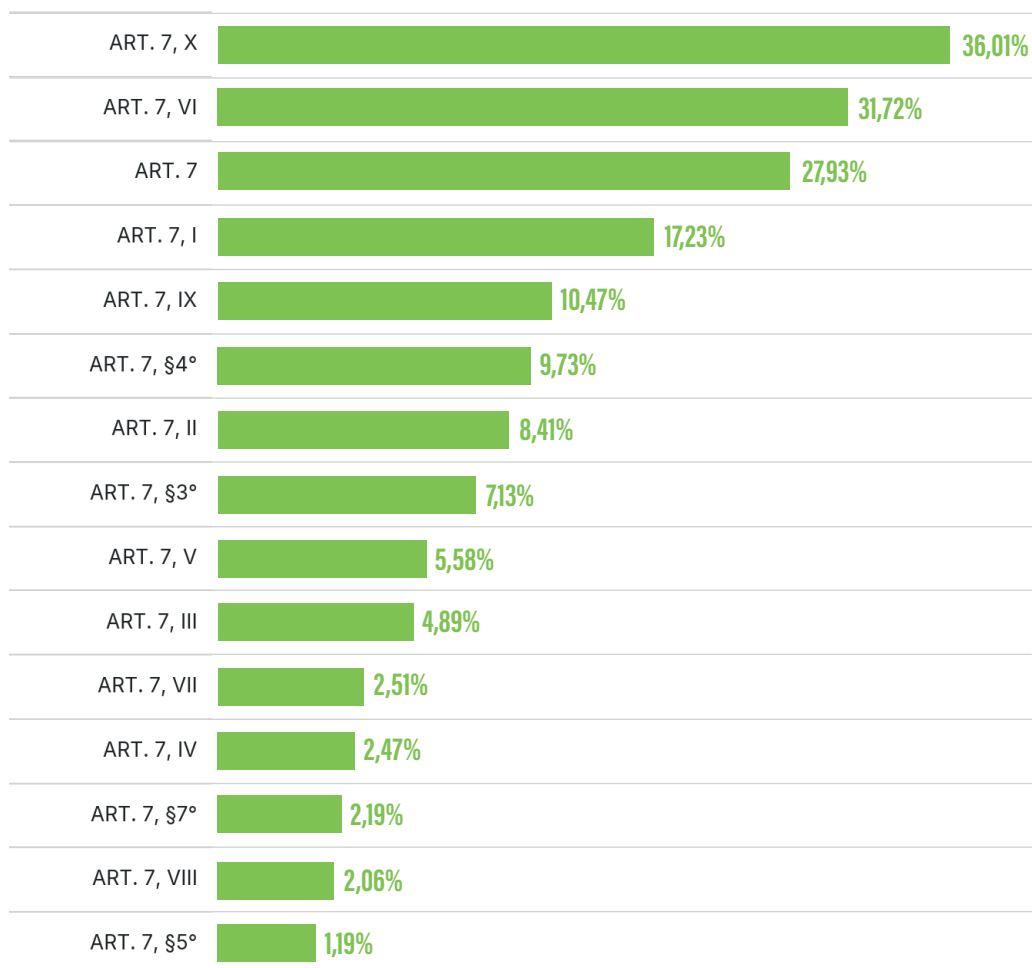
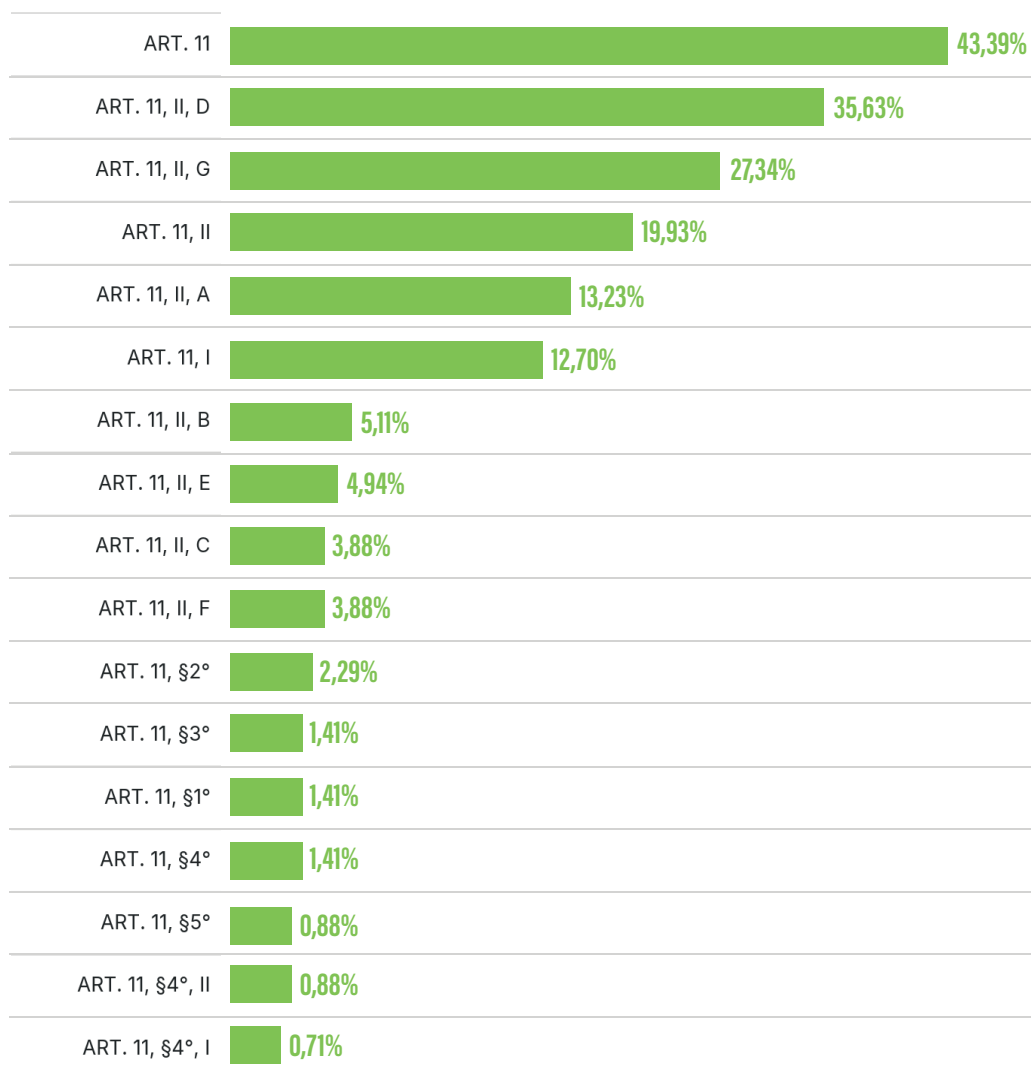


Tabela 18: Incisos e caput do art. 11 mencionados (%)



Do universo de 2.450 decisões relacionadas a bases legais, observa-se a prevalência de tribunais estaduais, em relação à Justiça Federal, Justiça do Trabalho e tribunais superiores, vide:

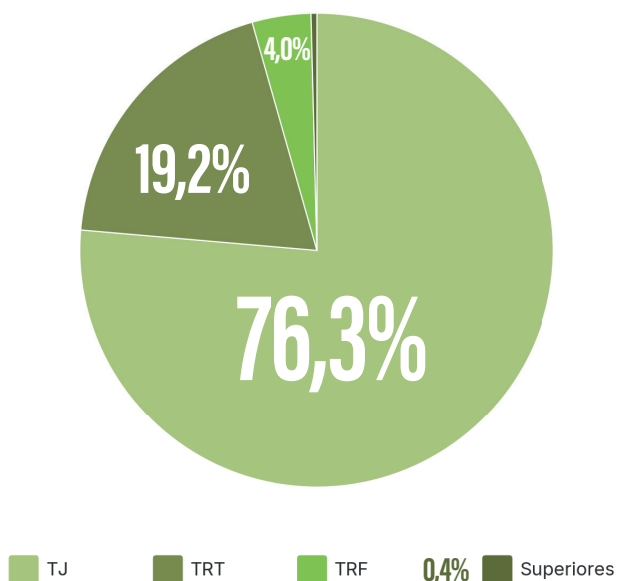


Gráfico 15: Tipo de tribunal mais frequente - Bases legais

Classificando o universo de decisões relevantes relacionadas a bases legais (2.450), decisões de primeira instância representam 70,08% (1.717), enquanto segundo grau seriam 29,55% (724) e tribunais superiores, 0,37% (9), vide gráfico:

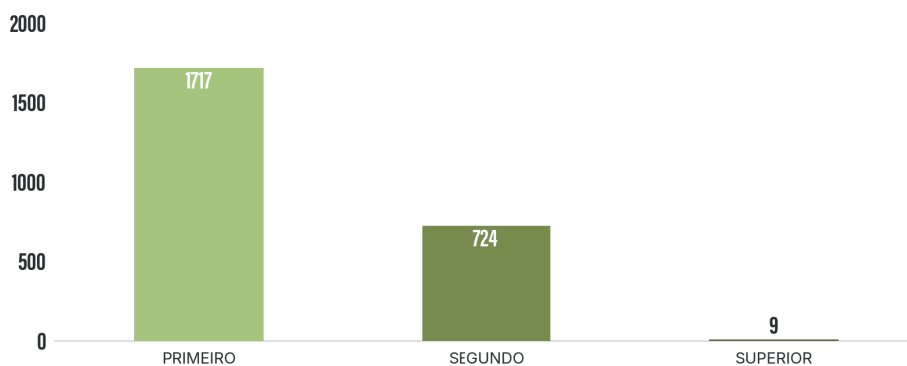


Gráfico 16: Instância mais frequente - Bases legais

Por fim, analisando o universo de decisões relacionadas a bases legais, os setores mais incluídos no polo ativo e passivo foram, respectivamente:

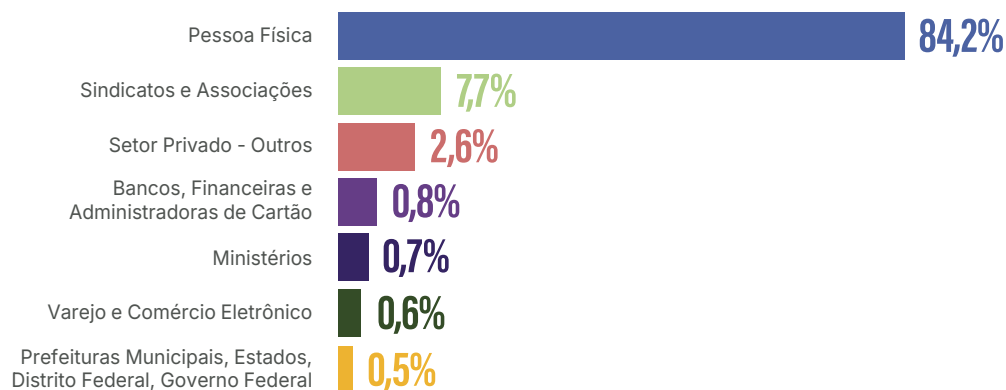


Gráfico 17: Setores mais frequentes polo ativo - Bases legais

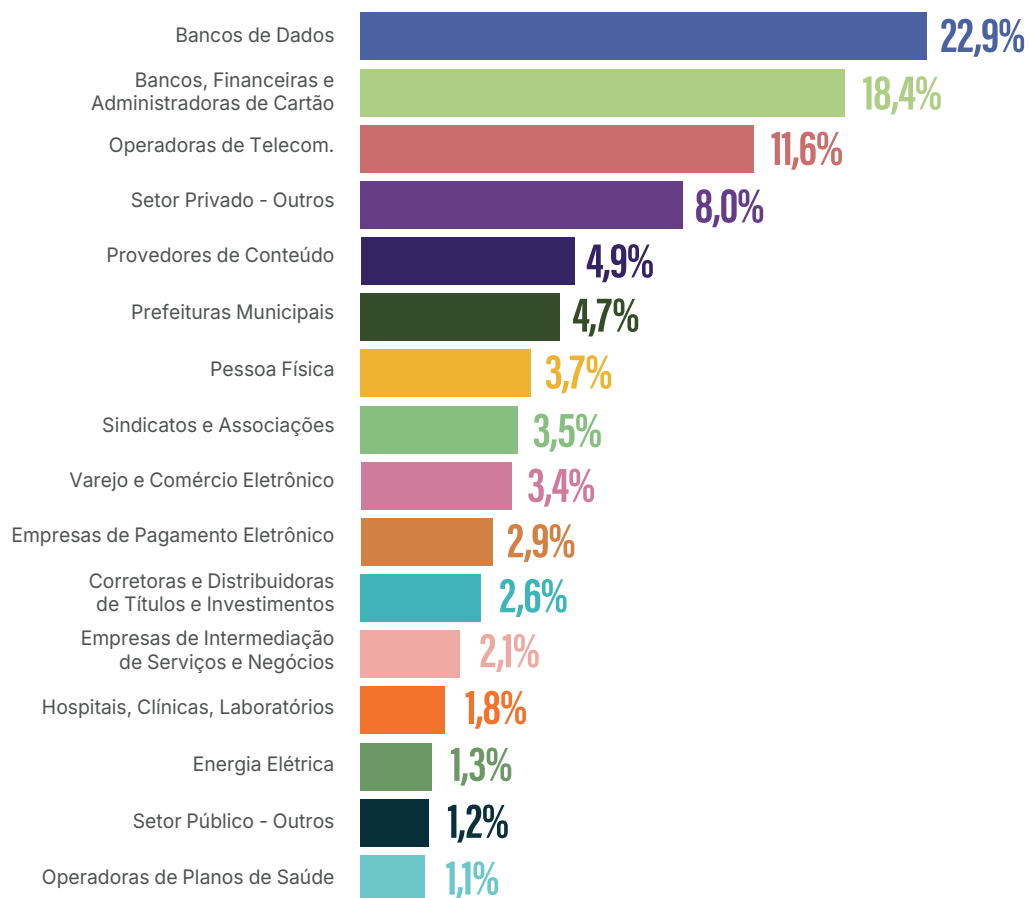


Gráfico 18: Setores mais frequentes polo passivo - Bases legais

i. Proteção do crédito (art. 7º, X) e Prevenção à fraude (art. 11, II, g)

Os casos que mencionam o artigo da base legal de proteção do crédito (art. 7º, X) envolvem, em sua maioria, ações em face de bancos de dados de cadastro e de consumidores (aproximadamente 60%). Nesse contexto, observa-se um número substancial de ações em que os titulares de dados pessoais invocam a LGPD para questionar a inscrição de seus dados pessoais em bancos de proteção ao crédito - alegando compartilhamento indevido de dados pessoais, comercialização e acesso não autorizado a dados pessoais. Nesse cenário, muitos dos autores requerem indenização por violação à LGPD, pedido observado em, ao menos, 266 dos casos.

Nota-se, ainda, que os §§3º e 4º do art. 7º são usualmente citados em casos relacionados ao cadastro positivo e à comercialização de dados. Os dispositivos são mencionados para reforçar a dispensa de consentimento nos casos de dados públicos ou tornados manifestamente públicos.

As menções ao art. 11, II, g (hipótese de prevenção à fraude), por sua vez, são majoritariamente feitas em conjunto com a base legal de proteção do crédito (art. 7º, X), de modo que é comum que a sua menção se dê de forma incidental, sem que de fato os dados pessoais tratados sejam dados pessoais sensíveis.⁵¹ A base legal de proteção do crédito segue integrando a Agenda Regulatória para o biênio de 2025-2026 da ANPD (tema 19), mas a expectativa é que o início do processo regulatório aconteça em até 2 anos.⁵²

Proteção do crédito (art. 7º, X)

- TJSP, 10165994520248260005, Des. Rel. Carlos Russo, data de julgamento 31/01/2025, disponível em: <https://www.jusbrasil.com.br/jurisprudencia/3023761452>.

51. Exemplificativamente: TJSP, 1025174-91.2024.8.26.0506, data de julgamento 04/12/2024, disponível em: <https://www.jusbrasil.com.br/jurisprudencia/3120603223>.

52. Disponível em: <https://www.in.gov.br/web/dou/-/resolucao-cd/anpd-n-31-de-22-de-dezembro-de-2025-6779500>

Proteção do crédito (art. 7º, X)

• TJSP,11707389220238260100, Des. Rel. Sergio da Costa Leite, data de julgamento 25/09/2025, disponível em: <https://www.jusbrasil.com.br/jurisprudencia/4968984559>.

• TJMG, 50054167520248130003, Des. Rel. Régia Ferreira de Lima, data de julgamento 25/09/2025, disponível em: <https://www.jusbrasil.com.br/jurisprudencia/tj-mg/4979118975>.

Prevenção à fraude (art. 11, II, g)

• TJSP, 10205017020248260016, Juíza Rel. Elisa Leonesi Maluf, data de julgamento 26/05/2025, disponível em: <https://www.jusbrasil.com.br/jurisprudencia/4137429879>.

• TRT-9, 8096520245090133, Juiz Rel. Maurício Mazur, data de julgamento 10/05/2025, disponível em: <https://www.jusbrasil.com.br/jurisprudencia/5458028773>.

• TJPI, 8047073320258180031, data de julgamento 25/09/2025, disponível em: <https://www.jusbrasil.com.br/jurisprudencia/4966911251>.

ii. Exercício regular de direitos (art. 7º, VI e art. 11, II, d)

O fundamento do exercício regular de direitos tem sido frequentemente utilizado em decisões da Justiça do Trabalho, para autorizar a produção de provas digitais, destacando-se os pedidos referentes à geolocalização. Os casos envolvem a necessidade de verificar fatos que digam respeito a direitos trabalhistas, como a efetiva jornada de trabalho, pedidos de horas extras etc.

A hipótese legal do exercício regular de direitos também é utilizada no âmbito civil e consumerista com o objetivo de embasar a produção de provas, incluindo pedidos de acesso de imagens de câmeras de monitoramento, além de outros documentos, no contexto desses processos.

Além disso, os artigos são mencionados em casos que discutem a publicação de dados pessoais de indivíduos a partir da publicidade de atos processuais, com titulares pedindo a anonimização ou pseudonimização dos dados, com referências à Resolução nº 121/2010 do CNJ. Esses casos são frequentes na Justiça do Trabalho e são discutidos na seção 4.c.iii.

- TJDFT, 7420753820238070001, data de julgamento 26/11/2024, Rel. Des. Maria Ivatônia, disponível em: <https://www.jusbrasil.com.br/jurisprudencia/2883453738>.

- TJRJ, 8038935520238190001, data de julgamento 12/09/2025, Rel. Des. Marianna Fux, disponível em: <https://www.jusbrasil.com.br/jurisprudencia/4855431426>.

- TRT-4, 253152320255040000, 27/09/2025, disponível em: <https://www.jusbrasil.com.br/jurisprudencia/5001727016>.

- TST, 105342620235150043, data de julgamento 21/03/2025. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/3294473805>.

iii. Consentimento (art. 7º, I e art. 11, I)

Com relação à base legal do consentimento, também é frequente a sua menção em contexto de inscrições de consumidores em plataformas de crédito, nas quais é discutida a exigibilidade do consentimento, vis a vis a base legal de proteção de crédito (art. 7º, X). Como discutido acima, grande parte das decisões acaba por concluir que a base legal de proteção ao crédito seria aplicável.

Ademais, observa-se que ao menos 65 decisões mencionaram o art. 8º, sem referenciar os arts. 7º ou 11, o que sinaliza a existência de debate sobre os requisitos de validade do consentimento a partir do art. 8º da LGPD.

Outros temas recorrentes nas decisões relacionadas aos referidos artigos incluem o compartilhamento de dados pessoais para fins de marketing, em que se discute, sobretudo, a validade do consentimento utilizado como fundamento para o compartilhamento ou utilização de dados por terceiros. Entre essas decisões, observa-se discussões sobre a validade de cláusulas contratuais com

hipótese de compartilhamento de dados, que, por vezes, são consideradas abusivas ou hipótese de consentimento inválido (por não ser específico ou por ser genérico). Também se destacam controvérsias envolvendo benefícios previdenciários, nas quais os tribunais frequentemente apontam a ausência de consentimento para o compartilhamento de dados de titulares de benefícios do INSS — situação que aparece, por exemplo, em processos envolvendo descontos indevidos.

- TJDFT, 7420753820238070001, data de julgamento 26/11/2024, Rel. Des. Maria Ivatônia, disponível em: <https://www.jusbrasil.com.br/jurisprudencia/2883453738>.

- TRT-15, 118365120245150077, data de julgamento 20/01/2025, Juíza Alzeni Aparecida de Oliveira Furlan, disponível em: <https://www.jusbrasil.com.br/jurisprudencia/trt-15/4991692944/inteiro-teor-4991692951>.

- TJMG, 50043030820248130514, 29/05/2025, disponível em: <https://www.jusbrasil.com.br/jurisprudencia/3944109872>.

- TJSP, 10004917420248260575, 14/04/2025, disponível em: Des. Rel. Mary Grün, <https://www.jusbrasil.com.br/jurisprudencia/tj-sp/3473595155>.

Colaciona-se, a seguir, exemplos a respeito das hipóteses legais mais citadas nas decisões analisadas.

Compartilhamento de Dados de Saúde entre Clínica e Plano de Saúde: Dever de assegurar a integridade das informações.

Dispositivos da LGPD citados: ART. 6º | ART. 6º, II | ART. 6º, III | ART. 7º | ART. 7º, V | ART. 11 | ART. 18, III

A decisão trata de ação ajuizada por menor representado por sua genitora contra clínica que compartilhou com o plano de saúde informações sobre supostas pausas no tratamento terapêutico, as quais posteriormente se revelaram imprecisas, o que teria prejudicado o paciente.

A controvérsia girou em torno da legalidade do compartilhamento dessas informações com o plano de saúde e da responsabilidade da clínica pelo repasse de dados incorretos. A discussão recaiu sobre dados pessoais sensíveis, especificamente dados de saúde de menor diagnosticado com TEA,

incluindo informações sobre frequência em sessões terapêuticas. A LGPD foi debatida sob a perspectiva da licitude do compartilhamento de dados entre prestadores de saúde e operadoras, bem como quanto aos limites impostos pelos princípios do art. 6º (finalidade, necessidade e minimização), pela disciplina do tratamento de dados sensíveis prevista no art. 11 e pelo direito de correção de dados inexatos assegurado no art. 18, III.

O tribunal reconheceu que a LGPD não impede o compartilhamento de dados necessários à execução do contrato de plano de saúde, mas entendeu que a clínica violou os deveres de exatidão e cuidado ao fornecer informações imprecisas, sem a devida verificação. Ao final, a ação foi julgada parcialmente procedente, com a consequente condenação da ré ao pagamento de indenização por danos morais.

TJAL, 0713126-31.2024.8.02.0058, Juiz: Helestron Silva da Costa. 8a Vara da Comarca de Arapiraca Cível Residual. Data de julgamento: 06/05/2025. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/tj-al/3621565846/inteiro-teor-3621565870>.

Uso de Imagens de Câmeras Condominiais e Exercício Regular de Direito.

Dispositivos da LGPD citados: ART. 1º | ART. 5º, I | ART. 7º, VI

Trata-se de ação de obrigação de fazer cumulada com indenização por danos morais ajuizada por condômina que alegou ter sido acusada, em reunião condominial, de realizar “transferências falsas”, o que teria atingido sua honra. Em pedido contraposto, alegou que a autora teria utilizado indevidamente imagens das câmeras de segurança do condomínio para instruir o processo, em suposta violação à LGPD.

A discussão envolvendo a LGPD se concentrou na utilização de imagens captadas por câmeras de segurança, qualificadas como dados pessoais, nos termos do art. 5º, I, da LGPD, para fins de instrução processual. O juízo destacou que o art. 7º, VI, da LGPD autoriza o tratamento de dados pessoais para o exercício regular de direitos em processo judicial, administrativo ou arbitral. Além disso, entendeu, no caso concreto, que as imagens foram juntadas exclusivamente como meio de prova, sem divulgação pública ou uso desproporcional, não havendo violação à legislação de proteção de dados.

Ao final, o Juizado concluiu pela inexistência de ato ilícito tanto na conduta da requerida, que agiu no exercício regular do direito de fiscalização condominial, quanto na utilização das imagens pela autora para fins de defesa em juízo. Assim, julgou improcedentes os pedidos autorais e o pedido contraposto, reconhecendo que não houve violação à LGPD.

TJAM, Processo no 0099529-74.2024.8.04.1000, Juíza: Articlina Oliveira Guimarães, Data de julgamento: 20/09/2025, 20o Juizado Especial Cível da Comarca de Manaus, Disponível em: <https://www.jusbrasil.com.br/-jurisprudencia/tj-am/4944210265/inteiro-teor-4944210267>.

4.3. Exercício de direitos do titular

Um dos pilares da proteção de dados é o reconhecimento de direitos a serem exercidos em nome das pessoas afetadas, os titulares dos dados, por uma atividade de tratamento feita por controladores, como por exemplo, empresas e órgãos públicos que processam informações pessoais para finalidades próprias a esses agentes. De forma geral, esses direitos estão previstos no Capítulo III da LGPD, apesar de haver previsões legais dispostas em outros capítulos da Lei.

Essa diferença na disposição dos direitos dos titulares pode ser explicada pelo fato de as espécies prescritas no Capítulo III da Lei serem direitos os quais os titulares exercem mediante pedido aos controladores, ao passo que os demais direitos do titular, como o estabelecido no art. 9º da Lei, devem ser cumpridos pelos controladores de forma espontânea, ou seja, sem prévio pedido do titular. Ainda, o Capítulo III também dispõe sobre o procedimento para o exercício do direito do titular peticionar à ANPD contra o controlador de dados (art. 18, §1º).⁵³

Vale notar que nem todos os dispositivos do Capítulo III criam espécies de direitos para o titular, já que este capítulo também contém regras procedimentais de como garantir o atendimento desses direitos. De forma específica, a LGPD cria as seguintes espécies de direitos dos titulares, que serão utilizadas como base para a análise do tema neste Relatório:

53. O direito de petição à ANPD não limita a possibilidade do titular peticionar judicialmente um pedido de exercício de direito dos titulares. Ou seja, mesmo antes de recorrer à ANPD, esfera administrativa, o titular pode requerer seu direito no âmbito judicial.

- Acesso a informações (art. 9)

- Informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados (art. 18, VII)

- Confirmação da existência de tratamento (art. 18, I)

- Acesso aos dados (art. 18, II)

- Oposição (art. 18, §2º)

- Correção de dados incompletos, inexatos ou desatualizados (art. 18, III)

- Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na LGPD (art. 18, IV)

- Portabilidade (art. 18, V)

- Revisão de decisões automatizadas (art. 20)

- Informações sobre decisões automatizadas (art. 20, §1º)

- Revogação do consentimento (art. 18, IX)

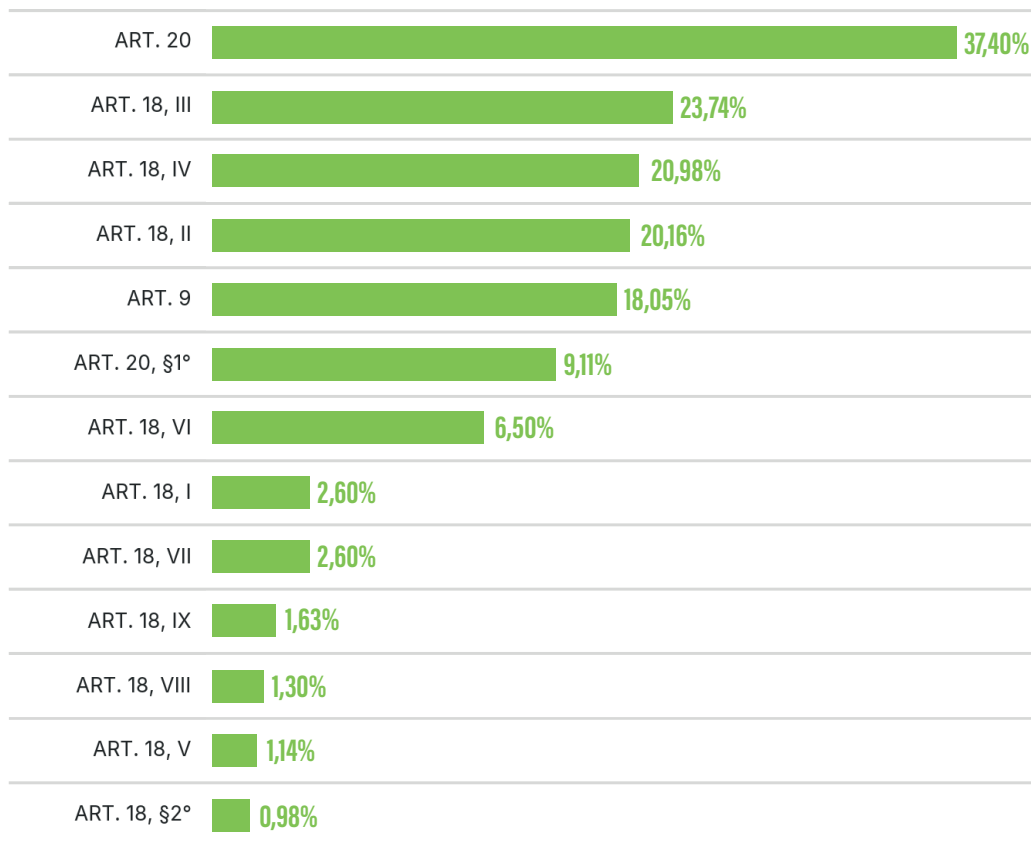
- Eliminação dos dados pessoais tratados com o consentimento do titular (art. 18, VI)

- Informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa (art. 18, VIII)

Nesta edição de 2025, das decisões que fazem parte do escopo da pesquisa, ou seja, das sentenças ou acórdãos relevantes que citam artigos da LGPD, que totalizaram 5.555 decisões, 2.107 abordam o tema de direitos dos titulares, cerca de 38%.

Ainda, entre as 5.555 decisões, 691 citam os artigos 9º, 18 ou 20 da LGPD, e 613 citam de forma explícita uma das espécies de direito do titular, ou seja, 11% das decisões abordam o tema. Nenhuma das decisões que citam artigos relacionados aos direitos dos titulares foi proferida por tribunais superiores. Ainda, cerca de 78% das decisões foram proferidas por Tribunais de Justiça, sendo cerca de 41% proferidas pelo TJSP, e 20% por Tribunais do Trabalho. O gráfico seguinte indica a porcentagem dos direitos previstos na LGPD mais citados no âmbito das decisões relevantes que mencionam os artigos relacionados aos direitos do titular:

Tabela 19: Artigos mais mencionados - Exercício de direitos do titular



Dentre as 613 decisões que citam de forma explícita uma das espécies de direito do titular, as seguintes informações podem ser extraídas:

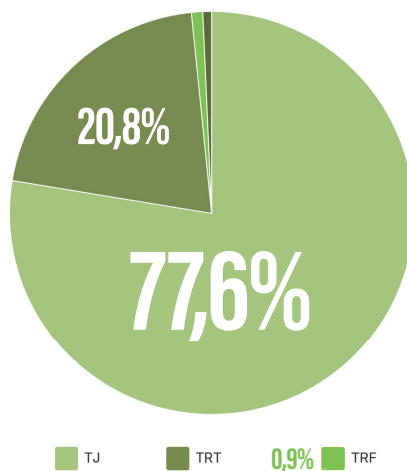


Gráfico 19: Tipo de tribunal mais frequente - Exercício de direitos do titular

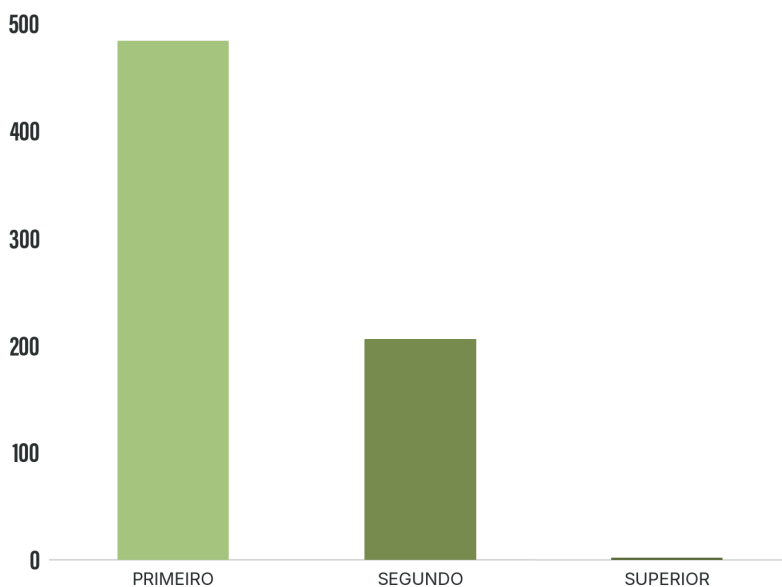


Gráfico 20: Instância mais frequente - Exercício de direitos do titular

Quanto ao setor envolvido nas demandas relacionadas ao direito dos titulares, em regra, o polo ativo das decisões é composto por pessoas físicas, cerca de 92% das decisões.

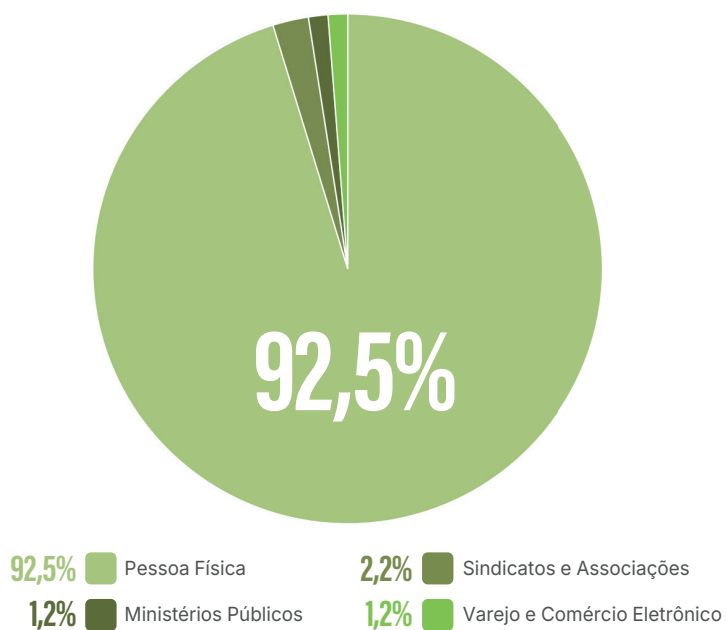


Gráfico 21: Setores mais frequentes polo ativo - Exercício de direitos do titular

Já o polo passivo é composto por diferentes setores, sendo possível consolidar o seguinte mapeamento com os cinco setores mais frequentes:

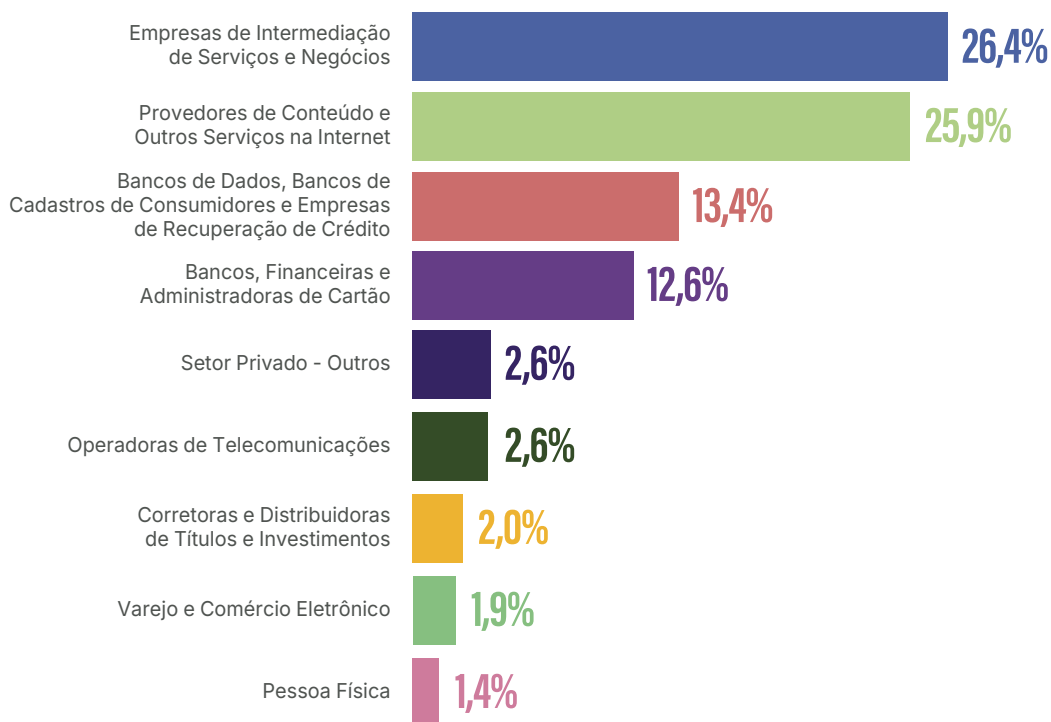


Gráfico 22: Setores mais frequentes pelo passivo - Exercício de direitos do titular

Dentre os direitos dos titulares mais frequentemente citados nas decisões, estão os direitos de: revisão de decisões automatizadas (230 decisões); correção de dados incompletos, inexatos ou desatualizados (144 decisões); anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na LGPD (127 decisões); acesso aos dados (121 decisões); seguido pelo direito a informações (109 decisões). Este Relatório se debruça sobre as três espécies de direitos mais frequentes.

i. Direito à Revisão de decisões automatizadas (art. 20)

A maior parte dos casos em que o direito à revisão foi debatido foi tratada em primeira instância nos Tribunais de Justiça (65%) ou nos Tribunais do Trabalho (34%). Os Tribunais de Justiça decidem sobre o direito de revisão de decisões automatizadas em diversos contextos. De forma geral, o artigo 20 é utilizado para tensionar assuntos como:

1.

Bloqueios e descadastramento de contas em aplicativos de transporte: decisões que versam sobre usuários, em regra motoristas ou entregadores de aplicativos, que têm contas banidas de plataformas por decisões automatizadas, alegando violação de termos de uso detectada por algoritmo, mas sem procedimento de revisão por um humano. Esses casos debatem a existência de lucros cessantes e pedido de reativação da conta.

2.

Bloqueios e invasões de contas em redes sociais e e-commerce: casos sobre usuários que têm contas desativadas ou suspensas por decisões automatizadas de moderação, sem prévia notificação ou possibilidade de defesa. Em regra, há pedido de indenização por danos morais e materiais, além de controvérsia sobre a responsabilidade do provedor.

3.

Sistemas de Proteção ao Crédito e Score: processos questionam como a pontuação para definir o risco de crédito do consumidor é calculada e por que o crédito foi negado sem uma explicação clara. Em regra, essas 94 decisões estão em contexto de questionamento sobre anotação negativa em plataforma de negociação ou a “comercialização de dados”, em que o tribunal indica para os direitos dos titulares como contrapeso para proteção dos titulares.

O emprego do art. 20 da LGPD pelos tribunais oscila no momento da fundamentação das decisões. Em uma parte importante dos processos, especialmente aqueles envolvendo bloqueio de contas, suspensão de perfis, descredenciamento de motoristas ou entregadores e outras restrições em plataformas digitais, o art. 20 aparece como fundamento mais direto para exigir transparência sobre a decisão automatizada, explicação das razões do bloqueio e a possibilidade de revisão humana da decisão.

Nesses casos, o tribunal trata o art. 20 de maneira mais "material", isto é, como base efetiva para enfrentar o problema do impacto de decisões automatizadas sobre a vida econômica ou social do titular. Essa interpretação está em linha com o precedente do STJ, Resp 2135783/DF, de junho 2024, que aponta que a plataforma, como controladora dos dados, deve fornecer, sempre que solicitado, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, já que afeta os interesses dos motoristas.⁵⁴

Por outro lado, em muitos outros processos, como os que tratam de score de crédito e cadastro restritivo, o art. 20 é citado no contexto da LGPD, mas o núcleo da solução judicial acaba se concentrando em outros direitos do titular, sobretudo os previstos no art. 18, com os direitos de acesso, correção, exclusão, bloqueio ou eliminação de dados. Em termos práticos, isso indica que os Tribunais de Justiça frequentemente usam o art. 20 como uma espécie de porta de entrada argumentativa para discutir proteção de dados, mas nem sempre desenvolvem uma análise aprofundada sobre revisão de decisão automatizada, deslocando a fundamentação para direitos mais tradicionais da matéria de dados pessoais.

Já no campo dos Tribunais do Trabalho, o tema de revisão com fundamento no art. 20 da LGPD é discutido em decisões em que 80% do polo passivo é composto por empresas de intermediação de serviços e negócios. O pano de fundo dessas decisões é a tentativa de reconhecimento de vínculo empregatício e o conseqüente pagamento de verbas trabalhistas e rescisórias entre motoristas e entregadores de aplicativos e essas plataformas de intermediação. O conflito agrava-se em razão de "bloqueios", "descadastramentos" ou "desativações" abruptas das contas desses trabalhadores nas plataformas.

54. STJ. REsp 2135783 - DF. Relator: Ministra Nancy Andrighi. 3a Turma. Data de Julgamento: 18/06/2024. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/stj/2939367384>

Os titulares alegam que essas dispensas foram executadas integralmente de forma automatizada por algoritmos, sem oportunidade de contraditório, sem transparência dos critérios e sem intervenção ou revisão humana.

Na maioria das decisões desse contexto trabalhista, a LGPD funciona como uma fundamentação acessória e incidental. Ela é utilizada especificamente para medir a legalidade do ato de desligamento e quantificar possíveis indenizações, mas não define, por si só, se há relação de emprego. O art. 20 da LGPD é utilizado como instrumento para exigir explicação ou revisão de bloqueios e desativações nas plataformas.

Nesse sentido, as decisões judiciais revelam diferentes desfechos para esse debate. Algumas reconhecem que o bloqueio automatizado sem chance de defesa ou revisão humana é um ato ilícito, condenando as plataformas ao pagamento de indenização por danos morais e determinando a reativação imediata da conta do trabalhador. Outras decisões indeferem os pedidos compensatórios alegando ausência de lastro probatório, indicando que o titular deveria provar que solicitou formalmente a revisão administrativa da decisão à plataforma antes de ingressar com a ação.

- TRT-13. 0000267-68.2025.5.13.0014. Juiz: Rodrigo Anderson Ferreira Oliveira. 6a Vara do Trabalho de Campina Grande. Data de Julgamento: 14/04/2025. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/3447058331>.

- TJAL. 0700693-66.2023.8.02.0078. Relator: George Leão de Omena. Turma Recursal Unificada. Data de Julgamento: 05/05/2025. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/3624834529>.

- TJRN. 0812989-59.2024.8.20.5004. Relator: Welma Maria Ferreira de Menezes. 3a Turma Recursal. Data de Julgamento: 05/05/2025. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/4733209285>.

- TRT-2. 1000794-38.2023.5.02.0706. Relator: Ricardo Apostólico Silva. 13a Turma. Data de Julgamento: 10/10/2024. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/3785208621>.

- TJSP. 1022727-59.2025.8.26.0001. Juiz: Aluísio Moreira Bueno. 3a Vara Cível do Foro Regional I - Santana. Data de Julgamento: 08/09/2025. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/4851988144>.

ii. Direito à correção de dados incompletos, inexatos ou desatualizados (art. 18, III)

O direito à correção de dados é a segunda espécie de direito mais citada nas decisões. Esse direito permite que o titular solicite a mudança dos seus dados pessoais registrados junto a um controlador por motivos de incompletude dessas informações, inexatidão ou desatualização. O conjunto de decisões que menciona o art. 18, III, é marcado por dois grandes blocos de contexto distintos.

O primeiro bloco reúne casos de contas e plataformas digitais, com destaque para invasão de conta, bloqueio/suspensão, recuperação de acesso e falha de segurança, por exemplo, e-mail, redes sociais e contas comerciais em plataformas. Nesses casos, o litígio costuma combinar obrigação de fazer, com o restabelecimento ou a recuperação da conta, com pedido de indenização, e a LGPD entra como base para discutir direitos do titular para alterar seus dados, que teriam sido manipulados erroneamente pelo agente invasor da conta. Nesse sentido, o direito de correção serviria para garantir o controle dos dados vinculados a uma conta.

O segundo bloco muito recorrente envolve o contexto de crédito, cobrança e negativação, especialmente ações de inexigibilidade de débito por prescrição, pedidos de retirada de apontamento em cadastros de inadimplentes e discussões sobre score de crédito. O problema jurídico gira em torno da permanência de dados desatualizados ou indevidos em bancos de dados e do impacto disso na vida civil do autor.

Em muitos casos, especialmente no bloco relacionado ao crédito e negativação, a fundamentação destaca que o titular deveria buscar antes a regularização perante o gestor do banco de dados (por exemplo, pedido administrativo prévio de exclusão/correção do apontamento). Assim, o art. 18, III é citado junto com esse dever de prévia solicitação, funcionando como base para discutir interesse de agir e a dinâmica entre esfera administrativa e judicial.

Em síntese, os tribunais têm aplicado o art. 18, III, não apenas para “corrigir um dado” no sentido formal, mas como fundamento mais amplo para impor regularização cadastral, retirada de informação indevida, atualização de registros e medidas de controle sobre dados pessoais, especialmente quando o erro ou a desatualização produz efeitos concretos, como a negativação, perda de acesso à conta, prejuízo funcional ou reputacional.

- TJSP. 1008658-82.2024.8.26.0348. Juiz: Anderson Fabrício da Cruz. 1a Vara Cível do Foro de Mauá. Data de Julgamento: 22/10/2024. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/2918240555_97.

- TJRN. 0800293-82.2025.8.20.5124. Juiz: Ana Cláudia Braga de Oliveira. 3o Juizado Especial Cível, Criminal e da Fazenda Pública da Comarca de Parnamirim. Data de Julgamento: 15/07/2025. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/4457869364>.

- TJSP. 1127196-87.2024.8.26.0100. Juiz: Regis de Castilho Barbosa Filho. 41a Vara Cível do Foro Central Cível. Data de Julgamento: 22/10/2024. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/3955984836>.

- TJMG. 5006690-64.2024.8.13.0362. Juiz: Vanessa Torzecki Trage. 1a Vara Cível e da Infância e da Juventude da Comarca de João Monlevade. Data de Julgamento: 25/08/2025. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/4570317256>.

ii. Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na LGPD (art. 18, IV)

A LGPD reconhece que o titular deve ter controle efetivo sobre o ciclo de vida de seus dados pessoais. Por isso, o art. 18, IV, garante o direito de solicitar a anonimização, o bloqueio ou a eliminação de informações que estejam sendo tratadas de forma inadequada, seja porque são desnecessárias, excessivas ou tratadas em desconformidade com a lei. Esse direito funciona como um mecanismo de correção e proteção, similar ao direito à correção previsto no art. 18, III, permitindo que o titular intervenha sempre que o tratamento ultrapassar os limites previstos pela LGPD.

No que diz respeito ao contexto comum dessas decisões, o padrão dominante gira em torno de contas e plataformas digitais, especialmente situações de invasão de contas, bloqueio, suspensão de perfis, falha na recuperação de acesso e omissão da plataforma em adotar providências. Nesses casos, o problema jurídico costuma combinar obrigações de fazer relacionadas ao restabelecimento de acesso, à recuperação de conta, à adoção de medidas de proteção com pedido de indenização por danos morais etc. Esse tema é semelhante aos

casos predominantes no debate do direito à correção de dados, com base no art. 18, III, da LGPD.

Um segundo grupo relevante de decisões encontra-se no âmbito de processos trabalhistas, nos quais o debate envolve a anonimização de dados em processos, a proteção da intimidade e os limites da publicidade processual, aproximando o art. 18, IV, de pedidos de sigilo, ocultação de nome e tratamento de dados em documentos judiciais. Nesses casos, o direito de anonimização é utilizado não em face da parte no processo, mas é um pedido processual sobre os critérios de publicidade de atos processuais para evitar a criação de “lista sujas”, ou seja, bancos de dados que processam informações de pessoas que foram reclamantes em ações trabalhistas. Com isso, a matéria de proteção de dados não constitui o objeto central do mérito da ação, sendo incidente e procedimental.

Quanto a este direito, os tribunais utilizam o art. 18, IV, da LGPD, como fundamento para medidas de contenção e saneamento do tratamento de dados, principalmente por meio de bloqueio, anonimização e, em menor número de casos, eliminação de dados. O art. 18, IV frequentemente aparece aplicado em conjunto com outros direitos do art. 18, especialmente de acesso e correção, o que revela uma prática jurisprudencial de leitura integrada dos direitos do titular: o tribunal não se limita a reconhecer abstratamente o direito à anonimização, bloqueio ou eliminação, mas o usa como base para impor providências concretas de regularização e redução do dano.

Em termos de tendência, isso indica que o art. 18, IV, tem sido mobilizado pelos tribunais, sobretudo quando há necessidade de interromper a exposição indevida, restringir a circulação dos dados ou neutralizar os efeitos do tratamento, com especial intensidade nos casos de plataformas digitais e nos pedidos de anonimização em processos judiciais.

- TJSP. 1129999-43.2024.8.26.0100. Juiz: Priscilla Miwa Kumode. 41a Vara Cível do Foro Central Cível. Data de Julgamento: 05/12/2024. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/2919561091>.

- TJSP. 1171801-21.2024.8.26.0100. Juiz: Mariana de Souza Neves Salinas. 31a Vara Cível do Foro Central Cível. Data de Julgamento: 19/09/2025. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/4937184195>.

- TRT-9. 0000804-30.2023.5.09.0084. Relator: Ilse Marcelina Bernardi Lora. 5a Turma. Data do julgamento: 26/11/2024. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/3019064656>.

- TJMG. 5270533-97.2023.8.13.0024. Juiz: Christian Garrido Higuchi. 33a Vara Cível da Comarca de Belo Horizonte. Data do julgamento: 23/05/2025. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/3875584035>.

A seguir, são apresentadas decisões que exemplificam as questões tratadas neste tópico quanto às espécies de direitos dos titulares.

Análise de dados interna. Revisão de decisão automatizada. Direito de acesso. Transparência

Dispositivos da LGPD citados: ART. 20 | ART. 20, §1º | ART. 9º | ART. 18

Trata-se de Ação de Indenização por Danos Morais ajuizada por pessoa física em face de empresa do setor de aluguel de carros. A autora realizou reserva online de veículo, recebeu confirmação, mas, ao comparecer à agência, teve a locação recusada sob a justificativa genérica de “análise de dados interna”. Ao solicitar esclarecimentos, a empresa alegou que a LGPD impediria a divulgação dos motivos da negativa. A autora pleiteou indenização por danos morais.

A recusa da locação foi fundamentada em “análise de dados interna”, indicando tratamento automatizado de dados pessoais. O ponto central foi a negativa da empresa em informar os critérios utilizados, invocando a própria LGPD como justificativa para a ausência de transparência. O juízo destacou que a lei não autoriza opacidade, mas, ao contrário, assegura ao titular direitos de acesso, informação e revisão de decisões automatizadas.

Dessa forma, o magistrado entendeu que a negativa da locação decorreu de decisão baseada em tratamento automatizado, e que a empresa recusou-se a informar os critérios utilizados, concluindo pela violação frontal aos direitos de transparência e controle do titular. A sentença enfatizou que a LGPD não pode ser utilizada como “escudo” para ocultar informações, mas sim como instrumento de proteção do cidadão contra decisões arbitrárias e obscuras.

O juízo julgou procedente o pedido da autora para reconhecer a violação

à LGPD, especialmente quanto à ausência de transparência e negativa de revisão de decisão automatizada, além de condenar a ré ao pagamento de danos morais, já que a empresa frustrou a legítima expectativa contratual e violou direitos fundamentais de proteção de dados, gerando constrangimento e insegurança jurídica à autora.

TJMG, 5031424-21.2023.8.13.0231, Juiz José Afonso Neto, Data de julgamento: 04/09/2025, 2a Vara Cível da Comarca de Ribeirão das Neves, Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/4780523888>.

Decisão algorítmica. Desativação automatizada de conta. Direito de revisão de decisão automatizada.

Dispositivos da LGPD citados: ART. 20 | ART. 20, §1º

Trata-se de Recurso Ordinário interposto por motorista de aplicativo contra um aplicativo de transporte, visando ao reconhecimento de vínculo empregatício, à declaração de nulidade da dispensa, à reativação de sua conta na plataforma e à condenação ao pagamento de indenização por dano moral. A sentença havia indeferido os pedidos.

A LGPD é discutida especificamente quanto à utilização de decisões automatizadas para desativação da conta do motorista. O Tribunal analisou a desativação sob a perspectiva do art. 20 da LGPD, que garante ao titular o direito de solicitar revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais, especialmente quando tais decisões afetem seus interesses. A exclusão do motorista da plataforma, sem contraditório e sem motivação adequada, foi considerada incompatível com essa garantia legal. Assim, a LGPD foi integrada à fundamentação trabalhista para reforçar a necessidade de transparência, possibilidade de revisão e respeito às garantias mínimas diante de decisões automatizadas com efeitos relevantes sobre direitos do trabalhador, como a sua própria subsistência.

Nesse sentido, o Tribunal articulou normas trabalhistas e a LGPD para reconhecer tanto o vínculo de emprego quanto a ilicitude da dispensa automatizada, assegurando proteção reforçada ao trabalhador frente à gestão algorítmica da prestação de serviços.

TRT-7, 0000652-54.2024.5.07.0002, Relator José Antônio Parente da Silva, Data de julgamento: 16/08/2025, 3a Turma, Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/trt-7/4514768922>.

Exclusão de dados pessoais. Obrigação de prestar informações. Origem dos dados. Compartilhamento de dados.

Dispositivos da LGPD citados: Art. 18, IV | Art. 18, VI | Art. 18, §6º

Trata-se de Recurso Inominado Paulo, interposto por pessoa física contra companhia de seguros e previdência. A autora alegou que nunca forneceu seus dados à ré, mas foi surpreendida com descontos relacionados a seguro, sustentando uso indevido de seus dados pessoais. Por isso, a parte autora requereu: (i) informações sobre a origem dos dados; (ii) eliminação dos dados pessoais; e (iii) indenização por danos morais. A sentença de primeiro grau julgou o pedido improcedente.

Nesta decisão, a LGPD é tensionada principalmente sob a ótica do direito do titular à eliminação de seus dados pessoais. A controvérsia não se concentrou na comprovação de vazamento ou fraude, mas no direito autônomo da titular de requerer a exclusão dos dados quando inexistente base legal para o tratamento. A autora fundamentou seu pedido no direito de eliminação previsto na LGPD, independentemente da demonstração de fraude.

Em síntese, o Tribunal deu parcial provimento ao recurso para reconhecer o direito à eliminação dos dados pessoais diante da ausência de base legal para seu tratamento, mas afastou a responsabilidade civil por danos morais por falta de prova da captação ilícita dos dados ou dano efetivo. A juíza determinou ainda a observância do § 6º do art. 18, quanto à comunicação da exclusão a eventuais agentes com quem os dados tenham sido compartilhados.

TJSP, 1002229-91.2024.8.26.0189, Relatora Flavia Beatriz Goncalez da Silva, Data de julgamento: 10/04/2024, Colégio Recursal dos Juizados Especiais, Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/2775060336>.

4.4. Responsabilidade

A análise sobre decisões que discutem responsabilidade delimitou-se àquelas que dizem respeito ao reconhecimento ou afastamento da responsabilidade dos agentes de tratamento no caso concreto, desde que a controvérsia subjacente tenha como contexto a discussão sobre violação à proteção de dados pessoais⁵⁵.

O tema segue presente na maior parte das decisões e é especialmente relevante para compreender como os agentes de tratamento têm sido responsabilizados pelo tratamento de dados em suas respectivas atividades. O Judiciário vem se debruçando sobre o tema de forma significativa, de modo que, do total de 5555 decisões que compõem o escopo da pesquisa, 2179 envolvem discussões afetas à responsabilidade dos agentes de tratamento.

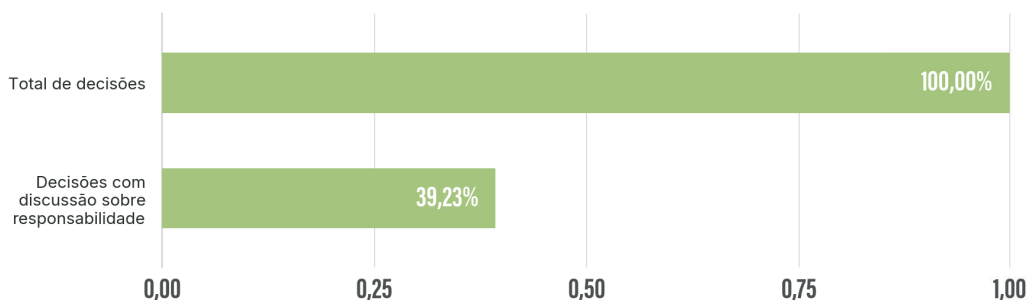


Gráfico 23: Total de decisões - Responsabilidade

55. Este mapeamento foi realizado com o auxílio da inteligência artificial, considerando que a controvérsia subjacente teria como contexto a discussão sobre violação à proteção de dados pessoais, sendo mapeadas aquelas decisões que pudessem reconhecer ou afastar a responsabilidade. O tema da responsabilidade pode incluir ou não a menção explícita de artigos que compõem a Seção III - Da Responsabilidade e do Ressarcimento de Danos, do Capítulo VI - Dos Agentes De Tratamento De Dados Pessoais, da LGPD.

Quanto às penalidades relacionadas à discussão de responsabilidade do agente de tratamento que foram aplicadas em razão de violação à proteção de dados, a maior parte das decisões concentraram-se na condenação de indenização por danos morais, seguida de indenização por danos materiais:

Tabela 20: Penalidades impostas c/c responsabilidade reconhecida

Penalidade imposta	%
Indenização por danos morais	32,80%
Indenização por danos materiais	20,70%
Obrigação de fazer	16,63%
Declaração de existência ou inexistência de uma relação jurídica	14,20%
Multa (em caso de descumprimento da obrigação de fazer/não fazer)	8,13%
Obrigação de não fazer	6,10%

Dentre as decisões que discutem responsabilidade, observa-se que os tribunais mais reincidentes são os tribunais de justiça, com presença predominante em 1ª instância:

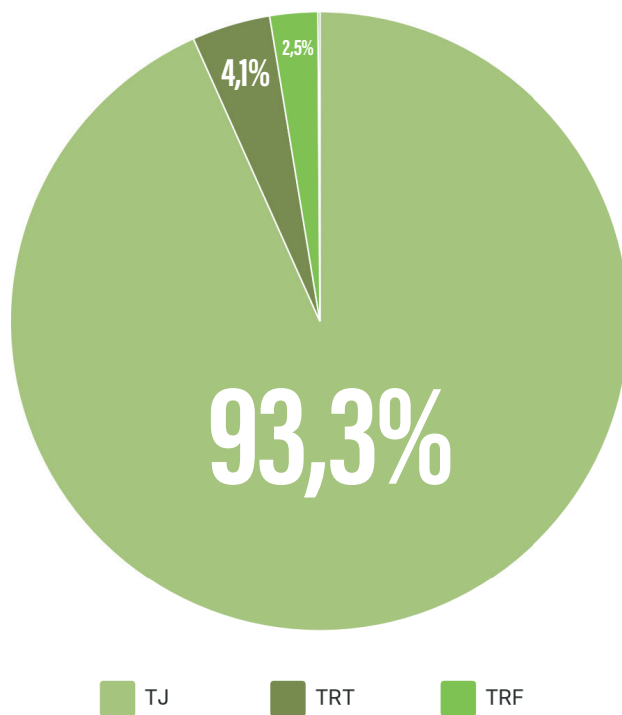


Gráfico 24: Tipo de tribunal mais frequente - Responsabilidade

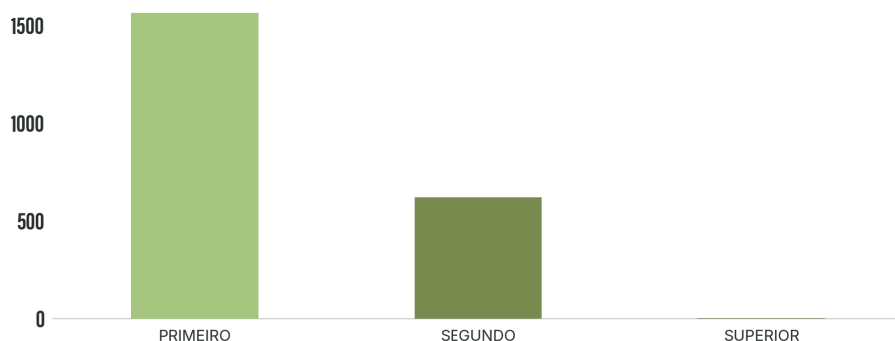


Gráfico 25: Instância mais frequente - Responsabilidade

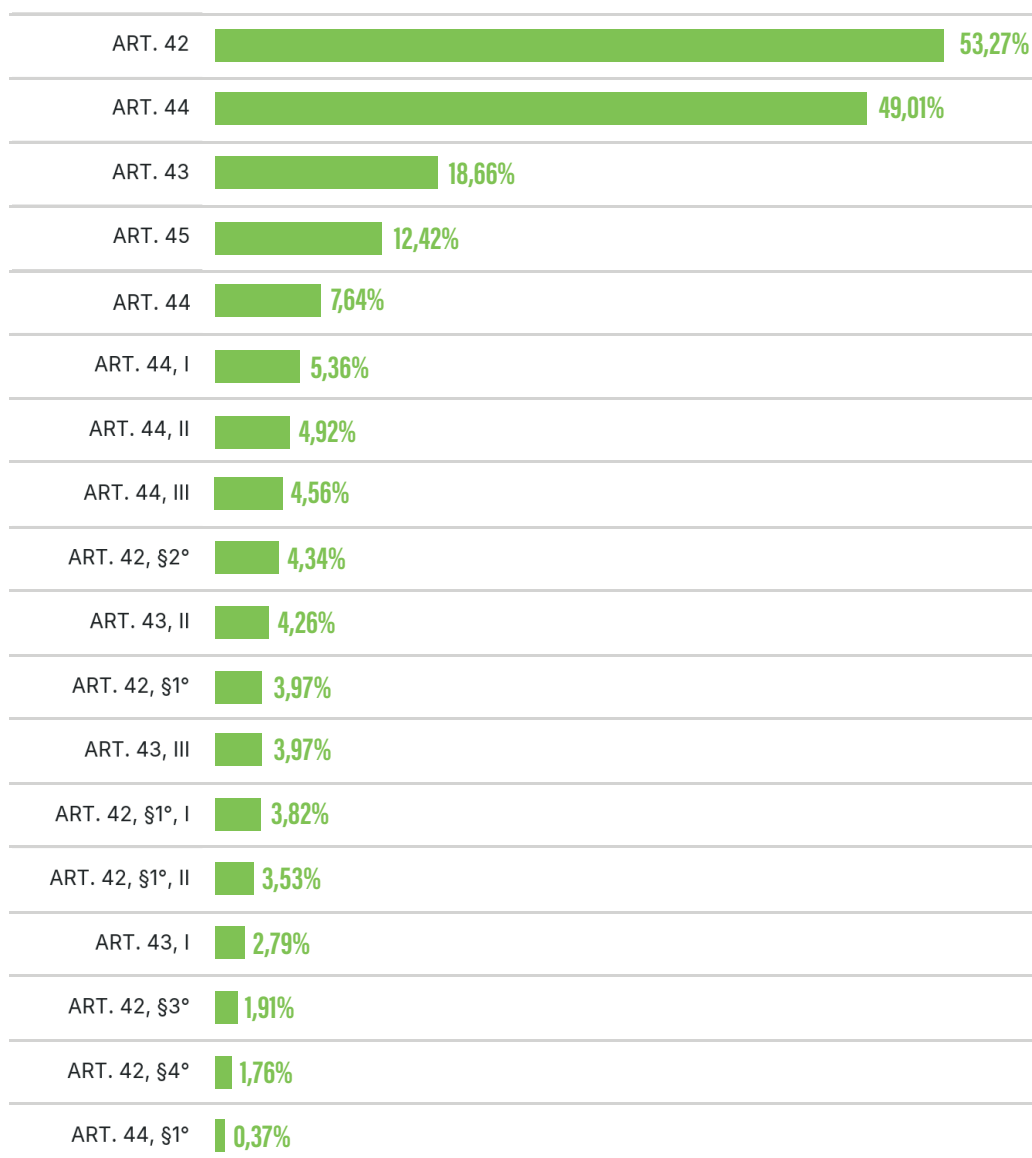
Tendo em vista que o recorte para a análise de discussão de responsabilidade não se restringiu às menções explícitas dos artigos da Seção III - Da Responsabilidade e do Ressarcimento de Danos, do Capítulo VI, da LGPD, destacam-se abaixo os dispositivos da LGPD mais mencionados nos casos envolvendo discussões de responsabilidade:

Tabela 21: Artigos mais mencionados - Responsabilidade

ART. 42	33,27%
ART. 44	30,61%
ART. 5, II	21,89%
ART. 46	17,44%
ART. 7, X	12,21%
ART. 43	11,66%
ART. 7	8,08%
ART. 6	8,08%
ART. 5, I	7,99%
ART. 45	7,76%
ART. 6, VII	6,52%
ART. 7, I	4,82%
ART. 44	4,77%
ART. 5	4,77%
ART. 11	3,90%

Quanto aos artigos específicos previstos na Seção III, do Capítulo VI, da LGPD, foram predominantes as menções aos arts. 42, caput e 44, caput:

Tabela 22: Artigos estritamente relacionados à Seção III, do Capítulo VI da LGPD - Responsabilidade



Quando verificados os polos mais frequentes afetos à discussão de responsabilidade, percebe-se que há uma predominância de ajuizamento de ações ou interposição de recursos por pessoas físicas, seguidas de outros agentes do setor privado e de sindicatos e associações:

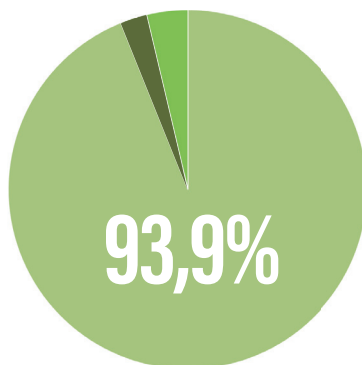


Gráfico 26: Setores mais frequentes polo ativo - Responsabilidade

Já quanto ao polo passivo, observa-se a predominância de três principais setores reincidentes em outros tópicos deste Relatório, como o setor de instituições financeiras (bancos, financeiras e administradoras de cartão), bem como de bancos de dados e cadastros de consumidores e empresas de recuperação de crédito, seguidas de provedores de conteúdo e serviços na internet:

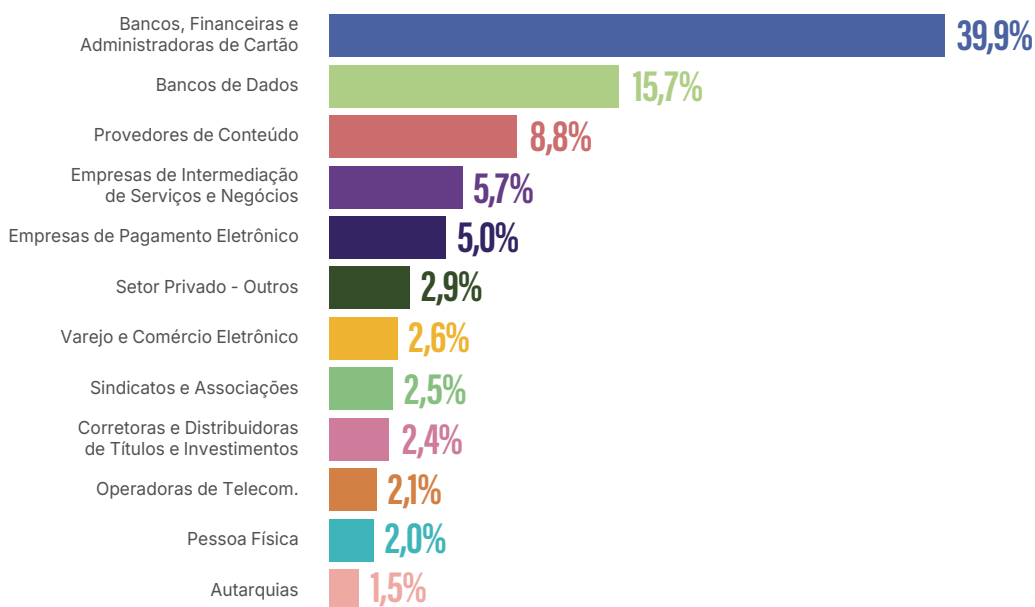


Gráfico 27: Setores mais frequentes polo passivo - Responsabilidade

No recorte adotado, evidenciaram-se os seguintes temas na discussão sobre responsabilidade:

1.

Bancos, Financeiras e Administradoras de Cartão: casos envolvendo fraudes bancárias, como golpes do boleto, falha de segurança da instituição financeira, compartilhamento/cessão de dados para proteção do crédito, bem como uma intersecção com negativação em plataformas de negociação e cobrança de débito.

2.

Bancos de Dados, Bancos de Cadastros de Consumidores e Empresas de Recuperação de Crédito: disputas relacionadas a compartilhamento de dados, inscrição e manutenção em cadastros, exercício de direitos de titulares, transparência e acesso aos dados.

3.

Provedores de Conteúdo e Outros Serviços na Internet: as decisões dizem respeito ao bloqueio/suspensão de conta em razão de invasão de conta, à remoção de conteúdos e ao fornecimento de dados dos titulares, bem como a falhas de segurança.

Além de outros setores relevantes, observou-se a presença considerável de decisões envolvendo o poder público, com destaque para demandas relacionadas especificamente ao INSS. As decisões relacionam-se, principalmente, com vazamento de dados de segurados e cobranças em associações sem consentimento, bem como abordagens comerciais a partir de dados do titular relacionados ao INSS.

i. Tendências sobre responsabilidade com menção ao art. 42 da LGPD

Dentre os dispositivos presentes na Seção de Responsabilidade da LGPD, aquele majoritariamente invocado, de forma substantiva, nas decisões sobre responsabilidade civil por violação à proteção de dados pessoais, é o art. 42 da LGPD. Tal artigo estabelece que o controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo. Nesse sentido, observou-se que o art. 42 da LGPD se destacou como fundamento normativo direto para fins de responsabilização do agente, enquanto a presença do art. 44 da LGPD foi, diversas vezes, vinculada nas decisões por intermédio de citações do REsp n. 2.077.278 SP, julgado pelo STJ, como parte do fundamento.

A responsabilidade dos agentes está intrinsecamente relacionada ao tópico de incidentes de segurança, assim como em outras edições. Nesse sentido, no recorte adotado nesta pesquisa, verificou-se o reconhecimento majoritário da responsabilidade do agente de tratamento por vazamentos que ocasionaram fraudes bancárias, bem como pela necessidade de restabelecimento de contas após invasão por terceiros em redes sociais. Além disso, também houve reconhecimento de responsabilidade de gestores de banco de dados por abertura de cadastros com base em informações de adimplemento, sem que houvesse consentimento prévio, bem como por disponibilização a terceiros consulentes de informações cujo compartilhamento seria, a princípio, restrito entre bancos de dados.

Nesse ponto, cabe mencionar que o art. 42 é mencionado em alguns casos em conjunto com o art. 46 da LGPD, destacando a necessidade de adoção de medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados.

- TJPR. 0001349-03.2022.8.16.0113. Juiz: Devanir Cestari. Data de Julgamento: 18/06/2025. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/tj-pr/4177115658/inteiro-teor-4177115666>.

- TJMG. 5006754-41.2024.8.13.0470. Juiz: José Rubens Borges Matos. Unidade Jurisdicional da Comarca de Paracatu. Data de Julgamento: 07/03/2025. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/tj-mg/3207828069/inteiro-teor-3207828078>.

- TJMT. 1077659-48.2024.8.11.0001. Juiz: Claudio Roberto Zeni Guimarães. 6o Juizado Especial Cível de Cuiabá. Data de Julgamento: 23/01/2025. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/tj-mt/3174199516/inteiro-teor-3174199524>

Tendo em vista que o tema de direito do consumidor é um dos predominantes nos tribunais quando se aborda a proteção de dados, percebe-se que o CDC é frequentemente abordado junto ao tema de proteção de dados pessoais. A menção em paralelo do art. 14 do CDC com o art. 42 também é utilizada para atestar a responsabilidade objetiva do agente por danos decorrentes de acesso indevido a dados pessoais.

- TJSP. 1004111-64.2024.8.26.0197. Juiz: Alexandre Pereira da Silva. Data de Julgamento: 25/02/2025. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/tj-sp/3277399339/inteiro-teor-3277399350>

- TJMG. 5007701-63.2023.8.13.0686. Relatora: Tereza Conceição Lopes de Azevedo. 2o Titular 1a TR Grupo Jurisdicional de Teófilo Otoni. Data de Publicação: 18/11/2025. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/tj-mg/3047303316/inteiro-teor-3047303317>.

- TJMG. 5078744-38.2025.8.13.0024. Juiz: Geraldo Claret de Arantes. 9a Unidade Jurisdicional Cível. Data de Julgamento: 23/05/2025. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/tj-mg/3925749253/inteiro-teor-3925749257>.

- TJMG. 5000477-26.2025.8.13.0647. Juiz: Fábio Henrique Vieira. Unidade Jurisdicional da Comarca de São Sebastião do Paraíso. Data de Julgamento: 23/09/2025. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/tj-mg/4965438326/inteiro-teor-4965438484>.

- TJMG. 5002016-94.2024.8.13.0054. Juiz: Luís Henrique Guimarães de Oliveira. Vara Única da Comarca de Barão de Cocais. Data de Julgamento: 13/11/2024. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/tj-mg/3314566862/inteiro-teor-3314566896>.

- TJCE. 3004332-24.2025.8.06.0071. Juiz: José Flávio Bezerra Moraes. 2a Vara Cível da Comarca de Crato. Data de Julgamento: 29/09/2025. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/tj-ce/5003787532/inteiro-teor-5003787534>.

Lado outro, também foram constatadas decisões que igualmente reconheceram em tese a responsabilidade disposta no art. 42, como responsabilidade objetiva, mas afastando-a no caso concreto. Essa constatação é relevante porque demonstra que o art. 42 não opera como fundamento automático de condenação, mas demonstra a importância que tem se dado a este dispositivo para compor o fundamento jurídico na análise da responsabilidade.

Por fim, cabe ressaltar que a menção ao art. 42 da LGPD para fins de afastamento da responsabilidade do agente de tratamento, ocorreu, principalmente, nos casos em que se reconhece a possibilidade de os bancos de dados manterem dados pessoais dos titulares em cadastros de inadimplentes para fins de proteção ao crédito, quando tais dados são utilizados em consultas por terceiros para fins de concessão de crédito.

- TJAM. 0074300-78.2025.8.04.1000. Juíza: Irlena Leal Benchimol. 5o Juizado Especial Cível da Comarca de Manaus. Data de Julgamento: 19/09/2025. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/tj-am/4947993481/inteiro-teor-4947993497>

- TJSP. 1029432-59.2024.8.26.0405. Juiz: Tobias Guimarães Ferreira. 1a Vara do Juizado Especial Cível. Data de Julgamento: 20/05/2025. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/tj-sp/3844660709/inteiro-teor-3844660725>

- TJPR. 0005486-05.2024.8.16.0098. Juíza: Joana Tonetti Biazus. Juizado Especial Cível de Jacarezinho. Data de Julgamento: 25/11/2024. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/tj-pr/5334739026/inteiro-teor-5334739028>

ii. Tendências sobre responsabilidade com menção ao art. 44 da LGPD

O art. 44 da LGPD dispõe sobre a irregularidade do tratamento de dados quando este deixar de observar a legislação ou quando não fornecer a segurança que o titular pode esperar, consideradas as circunstâncias relevantes do caso. O artigo guarda semelhança com o art. 14 do CDC, que estabelece a responsabilidade objetiva dos fornecedores por defeitos na prestação de serviço, quando o serviço não fornece a segurança que o consumidor pode esperar, levando-se em consideração as circunstâncias relevantes.

O art. 44 vem sendo abordado com frequência em paralelo ao art. 14 do CDC. A menção expressa entre o art. 14 do CDC e o art. 44 da LGPD, porém, tem sido observada reiteradamente em razão da menção do REsp n. 2.077.278 SP nos fundamentos da decisão. Cabe rememorar que no julgamento do REsp n. 2.077.278 SP, a Terceira Turma do STJ proferiu o entendimento de que o armazenamento de maneira inadequada, a possibilitar que terceiros tenham conhecimento de informações sigilosas e causem prejuízos ao consumidor, configura defeito na prestação do serviço, com base no art. 44 da LGPD e art. 14 do CDC. Ressalta-se, porém, que a jurisprudência citada é invocada porque inserida no contexto de discussão sobre violação à proteção de dados pessoais, o que evidencia a consolidação de tal referência do STJ nos julgados em 1ª e 2ª instância, como também foi indicado na edição passada do Painel LGPD.

- TJSP. 0001083-64.2025.8.26.0361. Juíza: Larissa Boni Valieris. Vara do Juizado Especial Cível e Criminal. Data de Julgamento: 19/03/2025. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/tj-sp/3277250558/inteiro-teor-3277250568>.

- TJAM. 0575056-54.2024.8.04.0001. Juiz: Roberto Hermidas de Aragão Filho. Data de Julgamento: 25/06/2025. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/tj-am/4135522410/inteiro-teor-4135522418>.

- TJPR. 0003857-33.2023.8.16.0194. Relator: Clayton de Albuquerque Maranhão. 4ª Câmara Cível. Data de Julgamento: 28/10/2024. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/tj-pr/2817409890/inteiro-teor-2817409893>.

- TJRJ. 0015246-95.2021.8.19.0066. Relator: Luiz Umpierre de Mello Serra. 21ª Câmara de Direito Privado. Data de Julgamento: 08/10/2024. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/tj-rj/3949024983/inteiro-teor-3949024986>.

- TJPR. 0005267-21.2024.8.16.0153. Juiz: Julio Cesar Michelucci Tanga. Juizado Especial Cível de Santo Antônio da Platina. Data de Julgamento: 12/05/2025. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/tj-pr/3940521224/inteiro-teor-3940521260>.

Ainda assim, de maneira desatrelada do art. 14 do CDC, o art. 44 da LGPD é suscitado para reconhecer a responsabilidade em casos decorrentes do vazamento de dados, principalmente nos casos que envolvem fraudes relacionadas às instituições financeiras e a redes sociais. No panorama geral, portanto, mesmo que a presença do art. 44 da LGPD nas decisões se dê principalmente via transcrição de citações jurisprudenciais, o resultado prevalecente é o de reconhecimento da responsabilidade do agente de tratamento por violação no tratamento de dados pessoais. Nos casos, são destacados a falha no dever de segurança dos agentes de tratamento em relação ao acesso de dados que deveriam ser restritos à relação entre o titular e o agente.

- TJDF. 0715047-16.2024.8.07.0016. Relatora: Marília de Ávila e Silva Sampaio. Segunda Turma Recursal. Data de Julgamento: 07/10/2024. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/2795810482>

- TJMG. 5023439-12.2024.8.13.0313. Juíza: Erica Climene Xavier Duarte. 1o JD da Comarca de Ipatinga. Data de Julgamento: 19/05/2025. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/tj-mg/3836228671/inteiro-teor-3836228675>

Por fim, o art. 44 da LGPD também é utilizado para afastar a responsabilidade, com menor frequência que para o reconhecimento da responsabilidade, ressaltando-se a exigência de demonstração do dano e do nexo de causalidade entre o fato ocorrido e o dano provocado. Há julgados que ressaltam, ainda, que além dos requisitos supracitados sobre responsabilidade civil, é necessário demonstrar lastro mínimo sobre a origem do vazamento.

- TRF-4. 5000323-32.2024.4.04.7112. Relator: Giovani Bigolin. 5a Turma Recursal do Rio Grande do Sul. Data de Julgamento: 28/03/2025. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/trf-4/3807688694/inteiro-teor-3807688704>.

- TJMT. 1000834-97.2024.8.11.0022. Juiz: Márcio Rogério Martins. Data de Julgamento: 04/09/2025. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/tj-mt/4784672632/inteiro-teor-4784672647>.

- TJDF. 0705090-70.2023.8.07.0001. Relator: Getúlio de Moraes Oliveira. 7a Turma Cível. Data de Julgamento: 25/09/2024. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/tj-df/2793573218/inteiro-teor-2793573219>.

iii. Aplicação do dano moral

No âmbito das discussões sobre a responsabilidade dos agentes de tratamento, um dos subtemas que se buscou mapear diz respeito aos eventuais danos morais decorrentes do reconhecimento da responsabilidade. Pelas tendências dessa edição, aproximadamente 45% das decisões que abordam o tema de responsabilidade impuseram condenação de dano moral. O reconhecimento bem como a rejeição da pretensão indenizatória dos danos morais alinha-se às situações de configuração ou inexistência da responsabilidade, respectivamente. Destacam-se as seguintes percepções:

1.

Natureza de dados pessoais gerais vs. dados sensíveis: A diferenciação entre a natureza do dado (se dado pessoal ou dado pessoal sensível) é tratado como eixo central para o afastamento ou reconhecimento do dano moral. Em geral, a diferenciação sobre a natureza dos dados é explicitamente citada quando se visa afastar o pedido de condenação por dano moral.

2.

Afastamento da condenação por danos morais: As decisões têm adotado como paradigma o AREsp 2.130.619/SP (Rel. Min. Francisco Falcão, Segunda Turma, j. 07/03/2023) para afastar a alegação de presunção de danos morais quando a falha no tratamento de dados envolve dados pessoais não sensíveis. Além disso, cabe mencionar que várias decisões mencionam esta particularidade mesmo quando já havia reconhecido, nos fundamentos da decisão, a ausência dos requisitos da responsabilidade. Ou seja, aborda-se a questão de diferenciação da natureza dos danos para reforçar a improcedência do pedido.

• TJSP. 1010489-21.2024.8.26.0008. Juíza: Roseleine Belver dos Santos Ricci. 1a Vara do Juizado Especial Cível. Data de Julgamento: 15/10/2024. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/tj-sp/2954121079/inteiro-te-or-2954121085>.

- TJPR. 0006126-91.2023.8.16.0017. Relator: Alexandre Barbosa Fabiani. 9a Câmara Cível. Data de Julgamento: 23/03/2025. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/tj-pr/3315256615>.

- TJAM. 0003721-97.2025.8.04.5400. Juiz: Marco Aurélio Plazzi Palis. 1o Juizado Especial da Comarca de Manacapuru. Data de Julgamento: 30/06/2025. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/tj-am/4158691627/inteiro-teor-4158691629>.

- TRT-15. 0010666-50.2023.5.15.0054. Relator: Renan Ravel Rodrigues Fagundes. 10a Câmara. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/trt-15/2850243041/inteiro-teor-2850243042>.

- TRT-4. 0021097-40.2024.5.04.0661. Relator: Ary Faria Marimon Filho. 1a Turma. Data de Julgamento: 06/08/2025. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/trt-4/4420251191/inteiro-teor-4420251202>.

3.

Reconhecimento da condenação por danos morais: Como supracitado, quase metade das decisões que versam explicitamente sobre responsabilidade reconheceram a condenação do polo passivo ao pagamento por danos morais.

4.

Dado pessoal: há uma significativa quantidade de casos que reconhecem o dano moral em casos de permissão de acesso ou compartilhamento por bancos de dados, com terceiros consultantes - que não sejam outros bancos de dados autorizados -, de dados pessoais sem consentimento. Tal posicionamento tem seguido o entendimento adotado pela 3a Turma, por maioria, no julgamento do REsp 2201694/SP.

- TJCE. 3004319-25.2025.8.06.0071. Juiz: José Flávio Bezerra Moraes. 2a Vara Cível da Comarca de Crato. Data de Julgamento: 01/10/2025. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/tj-ce/5013435759/inteiro-teor-5013435773>.

- TJMS. 0821670-77.2025.8.12.0001. Juiz: Renato Antonio de Liberali. 11a Vara Cível da Comarca de Campo Grande. Data de Julgamento: 23/09/2025. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/tj-ms/4963389147/inteiro-teor-4963389205>

- TJSP. 1006176-89.2024.8.26.0566. Relator: Eduardo Gesse. 28a Câmara de Direito Privado. Data de Julgamento: 18/10/2024. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/tj-sp/2797843690>

Além disso, também se verificou a condenação por danos morais por compartilhamento excessivo de dados pessoais, sem a aplicação de dano moral *in re ipsa*.

- TJCE. 3004654-44.2025.8.06.0071. Juiz: José Flávio Bezerra Moraes. Data de Julgamento: 30/09/2025. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/tj-ce/5013299677/inteiro-teor-5013299700>

- TJ-SP - Apelação Cível: 10227758920248260506 Ribeirão Preto, Relator.: Michel Chakur Farah, Data de Julgamento: 25/02/2025, 28a Câmara de Direito Privado, Data de Publicação: 25/02/2025. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/tj-sp/3089807716/inteiro-teor-3089807726>

- TJ-SP - Apelação Cível: 10290964320248260506 Ribeirão Preto, Relator.: Eduardo Gesse, Data de Julgamento: 15/04/2025, 28a Câmara de Direito Privado, Data de Publicação: 15/04/2025. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/tj-sp/3458669524>

5.

Dado pessoal sensível: No âmbito das decisões em que se discutiu a reparação por danos morais em razão da existência de dados sensíveis, verifica-se que a maior parte dos casos acolhe o pedido indenizatório, aderindo, muitas vezes, à teoria do dano moral *in re ipsa*.

- TRF-4. 50094028020244047000 PR, Relator.: GERSON LUIZ ROCHA, Data de Julgamento: 02/06/2025, 1a Turma Recursal do Paraná, Data de Publicação: 03/06/2025). Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/trf-4/3976477119/inteiro-teor-3976477126>.

- TJSP. 1201917-10.2024.8.26.0100. Juiz: Felipe Poyares Miranda. Data de Julgamento: 07/03/2025. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/3224996224>.

- TJSP. 1000345-54.2023.8.26.0062. Juiz: Vinicius Garcia Ferraz. 1a Vara. Data de Julgamento: 20/12/2024. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/2943797625>.

- TJAM. 0060040-93.2025.8.04.1000. Juiz: Mateus Guedes Rios. Data de Julgamento: 28/07/2025. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/tj-am/4313222199/inteiro-teor-4313222218>.

iv. Responsabilidade no âmbito do poder público

Embora em termos quantitativos o setor de "Autarquias" não esteja entre os setores mais suscitados, o tema foi destacado neste Relatório, dada a repercussão de relatos de vazamento de dados relacionados à Autarquia para além dos tribunais. Ressalta-se, por exemplo, que o INSS foi objeto de fiscalização pela Autoridade Nacional de Proteção de Dados (ANPD) por vazamento de dados cadastrais, fato que é também indicado em algumas decisões nos tribunais.

No âmbito do poder público, as decisões examinadas revelaram um padrão reiterado de demandas envolvendo o INSS. Foi constatado, inclusive no teor de algumas sentenças, o ajuizamento de ações com objetos semelhantes. O primeiro deles diz respeito a vazamento de dados pelo INSS e consequentes descontos indevidos em proventos previdenciários sem a anuência dos titulares, que expressam não terem autorizado a adesão a associações ou entidades representativas.

Além disso, também são reiterados os casos em que os titulares afirmam receber contatos de terceiros ofertando serviços, portados de informações vinculadas ao INSS, demonstrando, ainda, a proximidade do proferimento de

decisões de negativa ou deferimento de benefícios concedidos pelo INSS com tais importunações.

Um terceiro assunto recorrente nas lides relacionadas ao Instituto refere-se à oferta de crédito consignado aos titulares ou parentes de beneficiários do INSS por alegado vazamento de dados do INSS.

A responsabilidade do INSS foi afastada em um pouco mais da metade das decisões analisadas em que houve resolução do mérito, e aproximadamente 1/3 das decisões sobre o tema. Tal constatação foi percebida quando não havia nexos causais entre o uso irregular dos dados do titular e o alegado vazamento de dados pelo INSS, principalmente porque as informações não seriam restritas à relação entre o titular e a Autarquia ou porque já havia relação prévia com os terceiros que teriam tido acesso aos dados vinculados ao INSS.

Nos casos em que houve responsabilização da Autarquia, também em aproximadamente 1/3 das decisões, os tribunais mencionaram a correlação temporal entre as concessões/negativas de benefícios e os atos irregulares de terceiros, a especificidade do dado e a cadeia de custódia do INSS com tais dados. Cabe mencionar, porém, que em aproximadamente 1/3 das decisões, a responsabilidade não foi reconhecida por incompetência dos tribunais, mas as decisões ressaltaram a necessidade de os tribunais competentes examinarem possível responsabilização sob a LGPD por eventual falha do INSS em fiscalizar e impedir uso indevido de informações pessoais.

- TJCE. 3001149-44.2024.8.06.0018. Juiz: Magno Gomes de Oliveira. 4a Unidade dos Juizados Especiais Cíveis da Comarca de Fortaleza. Data de Julgamento: 26/05/2025. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/3871082761>.

- TJCE. 3000798-37.2025.8.06.0018. Juiz: Magno Gomes de Oliveira. 4a Unidade dos Juizados Especiais Cíveis. Data de Julgamento: 25/06/2025. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/4123555497>.

- TRF-3. 5036920-69.2023.4.03.6301. Relator: Juiz Federal Fernando Moreira Gonçalves. 1a Turma Recursal da Seção Judiciária de São Paulo. Data de Julgamento: 10/09/2025. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/trf-3/4927507378>.

- TRF-4. 5009402-80.2024.4.04.7000. Relator: Gerson Luiz Rocha. 1ª Turma Recursal do Paraná. Data de Julgamento: 02/06/2025. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/trf-4/3976477119/inteiro-teor-3976477126>.

v. Inversão do ônus da prova

Nas controvérsias que envolvem discussão sobre “responsabilidade”, um dos subtópicos verificado refere-se à menção ao art. 42, § 2º, da LGPD, que autoriza a inversão do ônus da prova em favor do titular quando houver verossimilhança da alegação, hipossuficiência probatória ou excessiva onerosidade na produção da prova. Trata-se de mecanismo especialmente importante, uma vez que boa parte das decisões tratam de relações entre um agente de tratamento que guardam dados pessoais e um titular mais vulnerável, que não detém acesso fácil a seus próprios dados que circulam no ambiente digital.

De qualquer maneira, a inversão não dispensa a demonstração dos pressupostos da responsabilidade civil, de modo que a parte autora continua obrigada a comprovar existência do dano e o nexo causal entre a falha no tratamento e o prejuízo alegado para atrair a responsabilidade do agente de tratamento.

- TJCE. 0206205-21.2023.8.06.0064. Juiz de Direito: Willer Sóstenes de Sousa e Silva. 3ª Vara Cível da Comarca de Caucaia. Data de Julgamento: 14/07/2025. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/tj-ce/4235012129/inteiro-teor-4235012153>.

- TJSP. 1003932-15.2025.8.26.0127. Juíza: Leila França Carvalho Mussa. 3ª Vara Cível. Data de Julgamento: 31/05/2025. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/tj-sp/3951538475/inteiro-teor-4056028065>.

vi. Excludente de responsabilidade

O art. 43 da LGPD estabelece as hipóteses de exclusão da responsabilidade dos agentes de tratamento. O dispositivo tem sido cotejado, sobretudo, com o art. 14, § 3º, do CDC, que prevê rol análogo de excludentes de responsabilidade no âmbito consumerista. Os casos em que o artigo é citado envolvem, geralmente, casos de fraudes e golpes financeiros, hipótese em que as institui-

ções financeiras buscam a incidência da culpa exclusiva da vítima.

- TJAL. 0744094-55.2023.8.02.0001. Juiz de Direito: Gustavo Souza Lima. 12a Vara Cível da Capital. Data de Julgamento: 06/05/2025. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/tj-al/3637780756/inteiro-teor-3637780843>

O dispositivo é citado, em geral, em contextos em que se reconhece a responsabilidade objetiva do agente de tratamento. Nestes casos, também são destacados os casos envolvendo o setor bancário.

- TJAL. 0700309-62.2023.8.02.0027. Juíza de Direito: Priscilla Emanuelle de Melo Cavalcante. Vara do Único Ofício de Matriz de Camaragibe. Data de Julgamento: 06/08/2025. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/tj-al/4965458734/inteiro-teor-4965458872>.

- TJAL. 0700025-66.2023.8.02.0023. Juíza de Direito: Priscilla Emanuelle de Melo Cavalcante. Vara do Único Ofício de Matriz de Camaragibe. Data de Julgamento: 18/12/2024. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/tj-al/2943280734/inteiro-teor-2943280739>.

Além disso, mesmo quando o conteúdo do art. 43 da LGPD não é desenvolvido da decisão, por tratar-se, por exemplo, de meras citações em jurisprudências, o dispositivo se insere em contextos em que são suscitadas as alegações sobre culpa exclusiva da vítima ou sobre culpa concorrente.

- TJ-PR 00031683320228160126 Palotina, Relator.: Helder Luis Henrique Taguchi, Data de Julgamento: 11/03/2025, 2a Turma Recursal, Data de Publicação: 12/03/2025. <https://www.jusbrasil.com.br/jurisprudencia/tj-pr/3224821973/inteiro-teor-3224822009>.

- TJ-PR 00014747020238160101 Jandaia do Sul, Relator.: Helder Luis Henrique Taguchi, Data de Julgamento: 13/12/2024, 2a Turma Recursal, Data de Publicação: 16/12/2024 - <https://www.jusbrasil.com.br/jurisprudencia/tj-pr/2939245218/inteiro-teor-2939245247>.

Há casos, porém, em que foram reconhecidas as excludentes de responsabilidade, especialmente em casos em que i) o fornecimento de dados pelo titular a terceiro caracteriza negligência do próprio titular dos dados, enquadrando-se na hipótese de culpa exclusiva da vítima ou ii) por ação criminosa ciber-

nética, em que se constata o acesso indevido dos dados do titular não por falha do agente de tratamento, mas por conduta ilícita de terceiro, atraindo a hipótese de fortuito externo:

- TJ-MG - Apelação Cível: 50005602420238130708, Relator.: Des .(a) Lílian Maciel, Data de Julgamento: 02/10/2024, Câmaras Cíveis / 20a CÂMARA CÍVEL, Data de Publicação: 03/10/2024. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/tj-mg/2776347546/inteiro-teor-2776347552>.

- TJ-DF 07473133820238070001 1973583, Relator.: AISTON HENRIQUE DE SOUSA, Data de Julgamento: 20/02/2025, 4a TURMA CÍVEL, Data de Publicação: 18/03/2025. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/tj-df/3509422229/inteiro-teor-3509422235>.

- TJSP. 1001627-64.2024.8.26.0007. Juiz: Alessander Marcondes França Ramos. 1a Vara Cível. Data de Julgamento: 11/03/2025. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/tj-sp/3254943095/inteiro-teor-3254943116>.

vii. Responsabilidade civil proativa ou ativa

A responsabilidade civil proativa ou ativa figura entre um dos temas de destaque desta edição, a qual, embora pouco mencionada nas decisões do escopo da pesquisa, demonstram a aplicação prática de conceitos doutrinários nos tribunais nacionais. A responsabilidade civil proativa ou ativa diz respeito à responsabilidade interpretada de forma sistemática a partir da LGPD, compreendendo que cabe ao agente de tratamento o dever não apenas de cumprir a lei, mas também provar que está em conformidade com o referido diploma legal. Além disso, em alguns casos a responsabilidade proativa foi ressaltada em contextos envolvendo relações consumeristas, e, ainda que suscitada a responsabilidade proativa, também se apontou a responsabilidade objetiva sob o viés do CDC, hipóteses em que se reconheceu a coexistência de ambas as vertentes.

No REsp 2.147.374/SP, de relatoria do Min. Villas Bôas Cueva, abordou-se de forma abrangente a estrutura normativa da LGPD, desde o seu fundamento constitucional (art. 5o, LXXIX, CF) até os princípios do art. 6o e os deveres dos arts. 46, 49 e 50. Na oportunidade, foi suscitado o referido conceito de responsabilidade civil proativa, destacando-se a necessidade de adoção de medidas eficazes de conformidade de programas de proteção de dados, bem como a

responsabilidade do agente de tratamento pelo tratamento irregular dos dados, à luz do art. 44, III, da LGPD, por ausência de fornecimento da segurança que o titular legitimamente poderia esperar. Além disso, na seara da responsabilidade, também é ressaltado no acórdão a inaplicabilidade ao caso da excludente de culpa exclusiva de terceiro (art. 43, III, da LGPD), uma vez que o agente de tratamento não logrou demonstrá-la nas instâncias ordinárias, tampouco comprovou a adoção de medidas de segurança adequadas, inviabilizando a aplicação da excludente.

- STJ. REsp: 2147374, Relator.: Ministro Ricardo Villas Bôas Cueva, Data de Publicação: 18/10/2024. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/stj/2932291599/inteiro-teor-2932291605>.

- TJPR. 0005673-13.2024.8.16.0098, Juíza Joana Tonetti Biazus, Juizado Especial Cível de Jacarezinho, Data de Julgamento: 10/03/2025. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/3284557328>.

- TJPR. 0005486-05.2024.8.16.0098, Juíza Joana Tonetti Biazus, Juizado Especial Cível de Jacarezinho, Data de Julgamento: 25/11/2024. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/tj-pr/5334739026/inteiro-teor-5334739028>.

Vazamento de dados pessoais. Responsabilidade. Instrução probatória necessária

Dispositivos da LGPD citados: ART. 42 | ART. 44.

Trata-se de ação de indenização por danos morais ajuizada em face de banco de dados, em que a autora alegou vazamento e comercialização indevida de seus dados pessoais no contexto do incidente amplamente divulgado em 2021, requerendo reparação por violação de direitos da personalidade. O juízo de primeiro grau extinguiu o feito sem resolução do mérito, por ausência de interesse processual, sob o fundamento de que não houve comprovação do vazamento nem demonstração de dano concreto.

O Tribunal, por sua vez, destacou o art. 42, relativo à responsabilização dos agentes de tratamento por danos decorrentes de uso indevido ou falha na proteção de dados pessoais, e o art. 44, que trata da ilicitude do tratamento irregular, concluindo que a LGPD prevê a responsabilidade dos agentes de tratamento por danos decorrentes de uso indevido ou falha na proteção de

dados pelo uso indevido ou falha na proteção, sendo desnecessária a comprovação prévia do dano para permitir o prosseguimento da ação.

Com base na teoria da asserção e na jurisprudência do STJ, o colegiado entendeu que a insuficiência de provas sobre o fato constitutivo do direito pode conduzir, ao final, à improcedência do pedido, mas não à extinção do processo por falta de interesse de agir. Ressaltou, ainda, que impedir a produção probatória em casos dessa natureza viola a inafastabilidade da jurisdição, o contraditório e a ampla defesa, sobretudo quando a pretensão envolve alegada violação a dados pessoais.

A sentença foi anulada, com determinação de retorno dos autos ao juízo de origem para regular prosseguimento da ação, a fim de que seja apreciado, no mérito, se houve tratamento irregular, vazamento de dados e responsabilidade civil da ré.

TJPE. 0001623-96.2024.8.17.3110, Rel. Des. Luciano de Castro Campos, 1a Turma da Câmara Regional de Caruaru, j. 02/04/2025. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/tj-pe/3357212254>.

Afastamento da responsabilidade. Medidas de segurança. Aplicativo de mensagens. Responsabilidade exclusiva de terceiros.

Dispositivos da LGPD citados: ART. 6º | ART. 42 | ART. 46, CAPUT | ART. 46, § 1º | ART. 46, § 2º | ART. 47 | ART. 50

Trata-se de ação movida por usuário de aplicativo de mensageria, vítima de fraudadores que “clonaram” o seu perfil, utilizando de sua lista de contatos e clientes para cobrar valores indevidos em nome do autor. Este alega que seus dados pessoais foram vazados e pleiteia o cancelamento de seu perfil e indenização por danos morais, uma vez que o aplicativo é empregado para fins empresariais.

Mediante a documentação analisada, o juízo entendeu que não ficou evidenciado um vazamento de dados pessoais imputável à ré e que não existia tecnicamente, medidas de segurança adicionais às já praticadas no estado da técnica que pudessem ser implementadas pela empresa, que fossem capazes de impedir ou reduzir o alcance do golpe sofrido pelo titular.

A decisão condenou à ré a cancelar definitivamente o perfil do autor no aplicativo, afastando qualquer imputabilidade de responsabilidade à ela, já que restou comprovada a aplicação de medidas de segurança adequadas pelo aplicativo e que a incumbência pelo fato gerador advém de responsabilidade

exclusiva de terceiro.

TJSP. 10294325920248260405, Relator Juiz: Tobias Guimarães Ferreira, Data de Julgamento: 26/04/2025, 1a Vara do Juizado Especial Cível – Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/3832437069>.

Responsabilidade proativa. Ausência de nexos causal. Dados pessoais comuns. Dano moral não configurado. Vazamento de dados.

Dispositivos da LGPD citados: ART. 2º, VI | ART. 5º, I | ART. 5º, II | ART. 42 | ART. 45

Trata-se de ação ajuizada em face de banco de dados, na qual a autora alegou que seus dados pessoais teriam sido vazados pela ré, com base em relatório indicando possível vazamento de dados na Dark Web.

A sentença analisou o regime de responsabilidade civil da LGPD em conjunto com o CDC, reconhecendo a responsabilidade objetiva nas relações de consumo (art. 42 da LGPD c/c art. 14 do CDC, este último, por força do art. 45 da LGPD). Contudo, destacou que, mesmo sob regime de responsabilidade objetiva, é imprescindível a comprovação do nexo causal entre a conduta do agente e o dano.

A decisão também abordou que o regime de responsabilização da LGPD seria a de responsabilidade ativa ou proativa, o que permitiria a aplicação da responsabilidade objetiva pelo CDC, garantindo-se a aplicação da LGPD ao rol de garantias e direitos do titular de dados pessoais e dos deveres dos agentes de tratamento de dados pessoais.

Também foi destacada a diferença entre dados pessoais comuns (art. 5º, I) e dados pessoais sensíveis (art. 5º, II), consignando que não havia evidências de vazamento de dados sensíveis, atraindo o julgado do STJ (AREsp 2.130.619/SP), para afastar a presunção de dano moral quando o dado envolvido é dado pessoal não sensível.

Por fim, no caso concreto, o Juízo suscitou que o próprio documento apresentado pela autora indicava expressamente que a ré apenas identifica vazamentos na Dark Web e não é fonte nem possui ligação com eventuais vazamentos indicados, não sendo possível estabelecer nexo de causalidade. Diante disso, o afastou-se a responsabilidade da ré por ausência de provas pelo alegado vazamento e ausência de dano moral.

TJPR, 0005673-13.2024.8.16.0098, Juíza Joana Tonetti Biazus, Juizado Especial Cível de Jacarezinho, Data de Julgamento: 10/03/2025. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/3284557328>

Dado pessoal vs. dado sensível. Dano moral não presumido. Vazamento de dados pessoais. Relação de emprego.

Dispositivos da LGPD citados: ART. 5º, I | ART. 5º, II

Trata-se de recurso ordinário em ação trabalhista na qual o autor alegou que, antes mesmo de ser formalmente comunicado de sua dispensa, recebeu ligação de escritório de advocacia que já tinha conhecimento de seu desligamento, evidenciando vazamento de dados pessoais pela empregadora.

Quanto a este ponto, o Tribunal analisou a questão diferenciando dados pessoais (art. 5º, I) de dados pessoais sensíveis (art. 5º, II). Concluiu-se que o nome completo e o número de telefone celular são dados pessoais, utilizados para identificação do indivíduo, e não dados sensíveis.

Com fundamento no entendimento do STJ (AREsp 2130619/SP), o TRT-15 entendeu que o vazamento de dados pessoais, embora seja falha indesejável no tratamento de dados, não gera dano moral presumível (*in re ipsa*). Assim, era ônus do trabalhador comprovar o dano efetivo decorrente da exposição dessas informações, o que não ocorreu nos autos. O mero contato para ingressar com ação trabalhista, embora violador dos deveres éticos da advocacia, não foi considerado apto a causar dor ou sofrimento indenizável.

Assim, o Tribunal deu parcial provimento ao recurso da ré para excluir a condenação por dano moral, reformando a sentença que havia fixado indenização de R\$10.000,00 por danos morais em razão do vazamento de dados.

TRT-15, ROT 0010666-50.2023.5.15.0054, Relator Des. Renan Ravel Rodrigues Fagundes, 10ª Câmara – 5ª Turma, Data de Julgamento: 08/11/2024, Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/trt-15/2850243041/inteiro-teor-2850243042>.

Responsabilidade objetiva do poder público. Vazamento de dados pelo INSS. Ligações de instituições financeiras. Dano moral configurado.

Dispositivos da LGPD citados: ART. 3 | ART. 5, X | ART. 6 | ART. 6º, I | ART. 7º, I | ART. 7º, § 5º | ART. 26, § 1º | ART. 42 | ART. 43, I | ART. 43, II | ART. 43, III | ART. 46 | ART. 46, §1 | ART. 46, §2 | ART. 47

Trata-se de ação de indenização por danos morais em face do INSS, na qual o autor alegou que, após a concessão de benefício de pensão por morte à sua mãe, passou a receber inúmeras ligações e mensagens de instituições financeiras ofertando crédito consignado, evidenciando o vazamento de dados do benefício previdenciário.

A decisão fundamentou-se na LGPD, destacando que as atividades de tratamento de dados pessoais devem observar a boa-fé e a finalidade legítima (art. 6º, caput e I), sendo necessário o consentimento do titular para compartilhamento com outros controladores (art. 7º, I e § 5º). Ressaltou que é vedado ao Poder Público transferir a entidades privadas dados pessoais constantes de suas bases de dados (art. 26, § 1º).

O Tribunal reconheceu a responsabilidade objetiva do INSS como controlador dos dados, com base no art. 42 da LGPD e destacou o dever de adoção de medidas de segurança (arts. 46 e 47 da LGPD).

O nexo causal foi demonstrado pelo lapso temporal entre a concessão do benefício e o início das abordagens, e pelo fato de múltiplas instituições financeiras, e não apenas uma, terem acessado os dados. O Tribunal ainda mencionou a punição aplicada ao INSS pela ANPD (Despacho Decisório no 1/2024/FIS/CGF) como fato público e notório do vazamento de informações. Recurso do INSS negado por unanimidade, mantida a condenação ao pagamento de R\$2.500,00 a título de danos morais.

TRF-3, RecInoCiv 0011678-64.2021.4.03.6302, Relatora Juíza Federal Lin Pei Jeng, 10a Turma Recursal da Seção Judiciária de São Paulo, Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/trf-3/2944963506/inteiro-teor-2944963514>.

Fraude bancária. Engenharia social.
Nexo causal afastado.

Dispositivos da LGPD citados: ART. 6º, VII | ART. 6º, VIII | ART. 44 | ART. 46

Trata-se de ação de indenização decorrente de fraude bancária, em que o representante da empresa autora foi contatado por pessoa que se apresentou como consultora do banco réu, a qual detinha informações do titular e o induziu a acessar site fraudulento e fornecer código token, viabilizando duas transferências bancárias.

A parte autora sustentou que houve vazamento de dados pelo banco, com violação dos princípios de segurança e prevenção da LGPD (art. 6º, VII e VIII), e que o réu falhou ao não detectar movimentação atípica.

O Tribunal citou o art. 44 da LGPD para afastar a responsabilidade, uma vez que não restou configurado o nexo causal entre a conduta do banco e o dano, pois os dados utilizados pelo fraudador não eram de tratamento exclusivo da instituição financeira.

Manteve-se a sentença de improcedência da ação, reconhecendo a ausência de vazamento de dados proveniente da ré, bem como a aplicação da culpa exclusiva do consumidor, com fundamento no CDC, afastando-se a responsabilidade da instituição bancária.

TJPR, Apelação 0026382-40.2022.8.16.0001, Relator Des. Luiz Cezar Nicolau, 15ª Câmara Cível, Data de Julgamento: 19/10/2024, Data de Publicação: 21/10/2024, Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/tj-pr/2802665276>.

4.5. Incidentes de Segurança

Incidentes de segurança permanecem como o principal vetor de materialização concreta da LGPD na jurisprudência brasileira. Diferentemente de debates mais abstratos sobre princípios ou bases legais do tratamento, os incidentes colocam o Poder Judiciário diante de eventos concretos (vazamentos, acessos indevidos, fraudes, uso irregular de dados), exigindo a aplicação direta dos dispositivos do Capítulo VII da LGPD.

Nesta edição, do universo de 5.555 decisões judiciais relevantes que mencionam dispositivos da LGPD, foi realizado recorte específico voltado aos incidentes de segurança, para examinar de que forma o Judiciário brasileiro vem aplicando os dispositivos relativos à proteção contra vazamentos, acessos não autorizados e demais falhas na segurança da informação. Para esse fim, foram selecionadas (i) decisões em que o vazamento e/ou uso indevido de dados pessoais foi um dos temas discutidos e (ii) decisões que, embora não tenham discutido a ocorrência do vazamento, mencionam dispositivos da LGPD relacionados à segurança dos dados, quais sejam os arts. 6º, VII, 44, 46, 47, 48 e 49. A aplicação desses critérios resultou no subconjunto de 2.405 decisões. Portanto, as considerações deste tópico serão realizadas com base neste recorte.

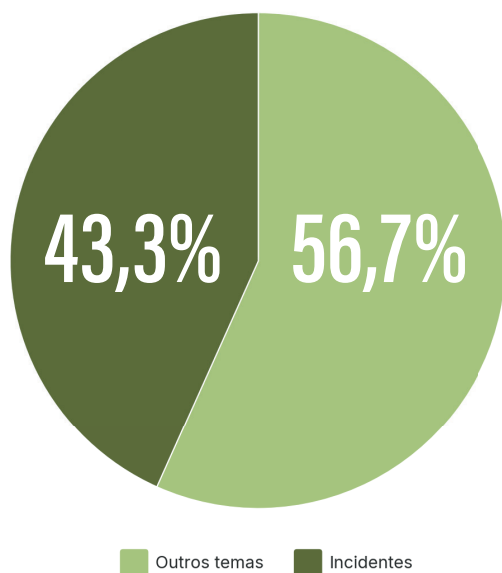


Gráfico 28: Recorte das decisões do tópico de incidentes de segurança

Dentre as decisões selecionadas, 1.795 (74,7%) são sentenças de primeiro grau e 605 (25,2%) são acórdãos. A quase totalidade dos precedentes provém da Justiça Estadual (2.267 decisões ou 94,3%). A Justiça Federal responde por 77 decisões (3,2%) e a Justiça do Trabalho por 56 decisões (2,3%). Os tribunais superiores aparecem de forma bastante residual, com 4 decisões (0,1%). Os tribunais com maior volume de casos são TJSP, TJMG e TJPR, concentrando 59,5% do recorte.

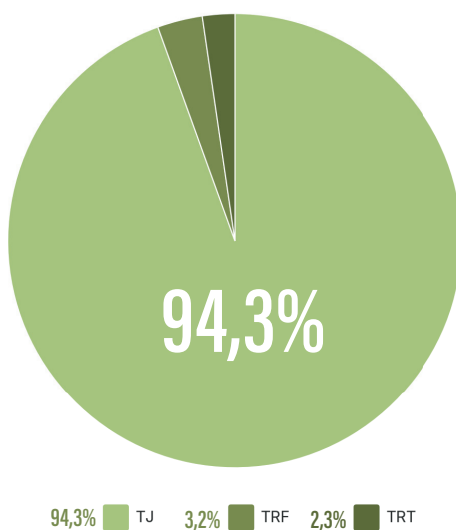


Gráfico 29: Tipo de tribunal mais frequente - Incidente de segurança

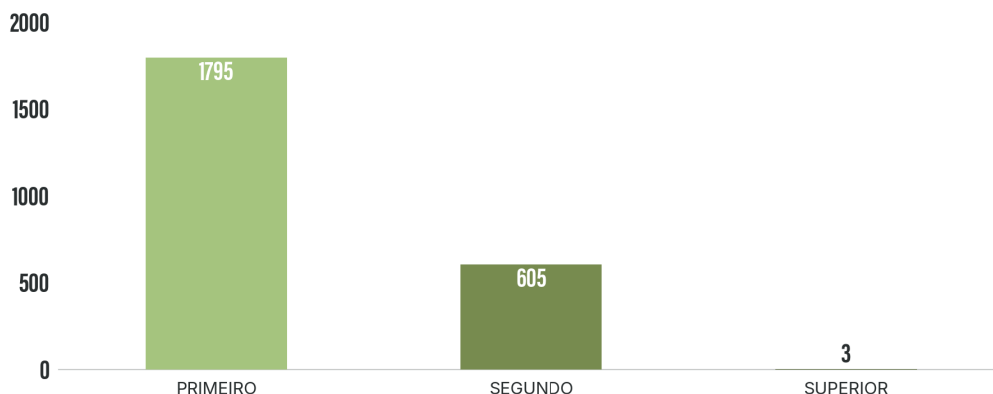


Gráfico 30: Instância mais frequente - Incidente de segurança

A análise do recorte demonstra ainda que a aplicação dos dispositivos da LGPD que abordam, de forma direta ou indireta, aspectos de segurança dos dados não se distribui de forma homogênea. Observa-se concentração expressiva nos arts. 44 e 46, seguidos do art. 6º, VII (princípio da segurança). Por outro lado, os arts. 47, 48 e 49 apresentam menor incidência. Em números absolutos, a distribuição é a seguinte:

Tabela 23: Artigos de segurança

Dispositivo	Nº de decisões
Art. 6º, VII (princípio da segurança)	210
Art. 44 (tratamento irregular)	766
Art. 46 (dever de segurança)	513
Art. 47 (armazenamento seguro)	48
Art. 48 (dever de comunicação)	364
Art. 49 (boas práticas e governança)	15

A análise do polo ativo revela concentração praticamente absoluta de demandas ajuizadas por pessoas físicas, o que confirma que a judicialização de incidentes é predominantemente individual e centrada na tutela de direitos subjetivos do titular. No polo passivo, há maior diversificação setorial, com predominância de instituições financeiras (bancos, financeiras e administradoras de cartão), que são seguidas pelos bancos de dados e cadastros de consumidores, autarquias federais (INSS etc.), provedores de conteúdo e serviços na internet, empresas de pagamento eletrônico e operadoras de telecomunicações. O panorama evidencia que os litígios se concentram em setores que operam grandes volumes de dados pessoais e financeiros ou que desempenham papel estratégico na infraestrutura digital e econômica, refletindo tanto a centralidade desses agentes nos fluxos informacionais quanto sua maior exposição a alegações de falha de segurança, tratamento irregular ou compartilhamento indevido de dados.

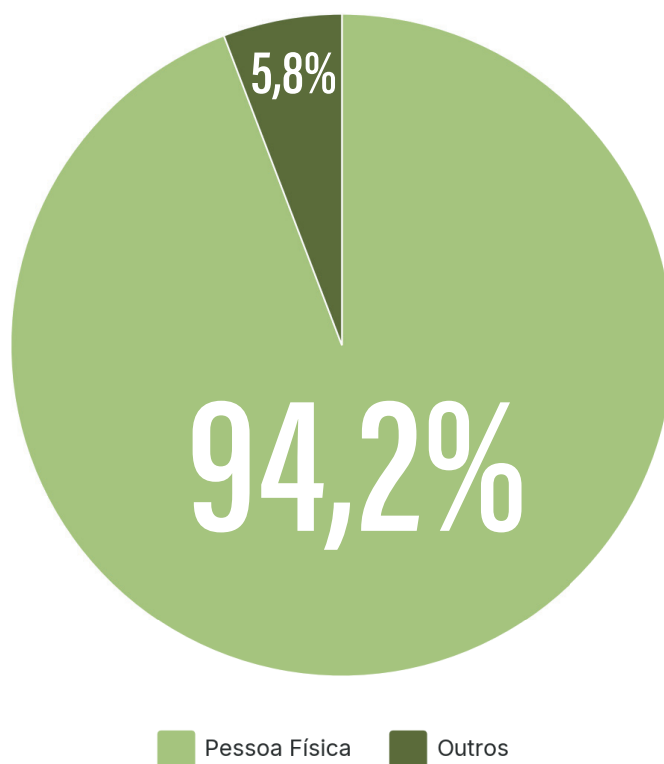


Gráfico 31: Setores mais frequentes polo ativo - Incidente de segurança

RELATÓRIO DO PAINEL NOS TRIBUNAIS

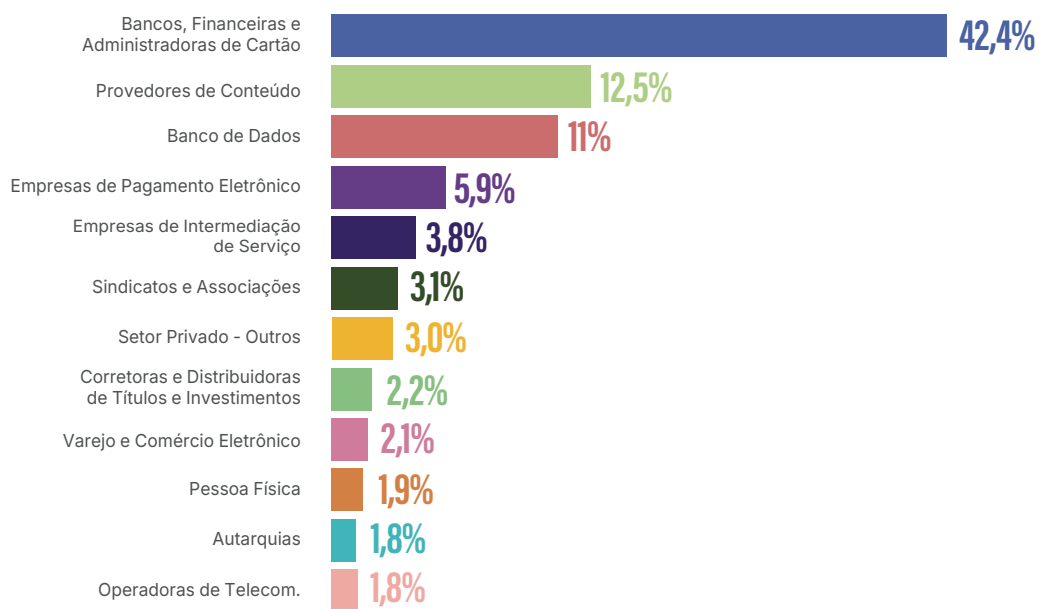


Gráfico 32: Setores mais frequentes polo passivo - Incidente de segurança

i. Tendências dos artigos relacionados aos incidentes de segurança

Esse padrão quantitativo também se reflete na forma como os dispositivos da LGPD são mencionados nos precedentes. Quando o incidente é discutido, há predominância do art. 44, que fundamenta o enquadramento da irregularidade do tratamento após a constatação do evento e funciona como a principal fonte normativa para a responsabilização civil das decisões classificadas como incidentes de segurança para fins deste tópico. A análise confirma essa centralidade: da amostra total de 5.555 decisões da pesquisa, o art. 44 foi mencionado em 738 (14,29%), percentual que sobe para 33,02% no recorte de decisões relacionadas a incidentes de segurança. O dispositivo, portanto, não é apenas frequentemente citado na jurisprudência em geral, mas vem se consolidando como verdadeira bússola nos casos de vazamento e uso indevido de dados.

Qualitativamente, as menções ao art. 44 seguem padrão relativamente estável: (i) discute-se a ocorrência do vazamento, fraude, acesso indevido; (ii) discute-se a existência de falha na proteção dos dados; e (iii) analisa-se se há tratamento irregular, nos termos do art. 44. Assim, o dispositivo opera como cláusula geral de imputação da ilicitude após a constatação do evento, sendo majoritariamente mencionado quando o incidente é reconhecido e raramente quando a ocorrência é afastada. Frequentemente articulado com o regime de responsabilidade civil (sobretudo em conjunto com o CDC), o art. 44 cumpre função de qualificação jurídica do fato, ainda que sem aprofundamento técnico a respeito do conteúdo concreto do dever de segurança mencionado no dispositivo.

O art. 46, por sua vez, é invocado como fundamento do dever de segurança, isto é, da obrigação de adotar medidas técnicas e administrativas aptas a proteger os dados contra acessos não autorizados ou situações ilícitas. Foi mencionado em 514 decisões, cerca de 9,2% da amostra total de decisões e em aproximadamente 21,38% do recorte de incidentes. Embora a presença seja expressiva, permanece inferior à do art. 44, indicando que o Judiciário tende a qualificar o evento como tratamento irregular com maior frequência do que a desenvolver, de maneira autônoma e aprofundada, os parâmetros técnicos do dever de proteção.

A aplicação do art. 46 ocorre, em geral, em dois contextos: para (i) fundamentar a responsabilização quando o Judiciário entende que está demonstrada a falha na segurança; ou (ii) afastar a responsabilidade quando não há prova

de que o incidente decorreu de conduta imputável ao agente. Em ambos os casos, o art. 46 funciona como parâmetro abstrato cuja violação depende de comprovação concreta. Contudo, há baixa densidade técnica na sua utilização: raramente há discussão estruturada sobre os padrões mínimos de segurança da informação, controles de autenticação, criptografia, segregação de funções e/ou políticas de resposta a incidentes. O dispositivo é frequentemente citado de forma genérica, sem critérios objetivos para aferir a suficiência das medidas adotadas.

O art. 48, relativo ao dever de comunicação do incidente à ANPD e aos titulares, surge de maneira bem residual. Foi mencionado em apenas 41 decisões (0,73% da amostra total e 1,7% do recorte de incidente), concentradas majoritariamente em primeiro grau e sem consolidação interpretativa uniforme. Mais relevante que o número absoluto é o padrão qualitativo: o art. 48 raramente constitui um fundamento jurídico autônomo da condenação, sendo geralmente mencionado de maneira acessória, na enumeração dos dispositivos supostamente violados. Ainda, assim como a ausência de notificação não é tratada como fundamento suficiente, por si só, para a responsabilização, a comunicação tempestiva não é vista como elemento capaz de afastá-la quando o vazamento é reconhecido.

Situação semelhante se observa em relação aos arts. 47 e 49, mencionados em só 48 e 15 decisões, respectivamente. A menção residual dos dispositivos evidencia que a jurisprudência permanece centrada na ocorrência do evento e nonexo causal, com baixa incorporação da dimensão procedimental e organizacional do regime de segurança estruturado pela LGPD.

Em síntese, as decisões analisadas indicam que o regime jurídico dos incidentes vem sendo aplicado sob a lógica da irregularidade consumada e da reparação do dano. Enquanto os arts. 44 e 46 são mencionados em um número maior de decisões, especialmente nas em que há reconhecimento de responsabilidade, os arts. 47, 48 e 49 têm aplicação limitada, revelando menor desenvolvimento da dimensão preventiva na jurisprudência brasileira atualmente.

Além do padrão observado na aplicação dos dispositivos da LGPD, a análise das decisões revela que a interpretação judicial também varia conforme o tipo de incidente discutido. A natureza do evento alegado influencia diretamente a avaliação da falha de segurança, do nexocausal e, em última instância, da própria responsabilização do agente de tratamento.

ii. Principais tipologias de incidentes de segurança

No recorte analisado, os incidentes são majoritariamente construídos a partir de narrativas relacionadas a fraudes e engenharia social. Eles raramente aparecem como falha sistêmica abstrata ou descumprimento estruturado de governança. Em geral, o incidente é apresentado como evento concreto, associado à atuação de terceiros. As principais tipologias identificadas evidenciam esse padrão.

Fraudes e golpes

O conjunto mais recorrente de decisões envolve fraudes através do uso indevido de dados pessoais em contextos de engenharia social, golpes digitais, boletos fraudados, transferências via PIX, clonagem de cartão e, recentemente, fraudes com biometria ou autenticação digital. Tais casos compartilham o seguinte pano de fundo: terceiro que usa dados pessoais da vítima para conferir verossimilhança à fraude e viabilizar um prejuízo patrimonial. A controvérsia, nestes casos, tende a se concentrar na origem dos dados utilizados pelo fraudador e na distinção entre dados cadastrais (como nome, CPF, telefone, e-mail), considerados amplamente acessíveis, e dados operacionais ou contratuais específicos, como número de benefício previdenciário, limite de crédito, valor exato de parcelas, histórico de transações ou informações internas da conta.

Quando o fraudador demonstra conhecimento de dados individualizados e vinculados à relação contratual, os tribunais tendem a presumir falha na proteção dos dados, reconhecendo irregularidade do tratamento com base no art. 44 da LGPD, frequentemente aplicado com o CDC. Com isso, o uso indevido é interpretado como um indício suficiente de vulnerabilidade da base do fornecedor. Por outro lado, quando os dados são genéricos e/ou passíveis de obtenção por múltiplas fontes (como redes sociais, cadastros públicos e/ou vazamentos não atribuídos ao réu), há maior propensão ao afastamento da responsabilidade, sob o argumento de ausência de provas donexo causal e de inexistência de demonstração de vazamento interno.

Nos casos de boleto fraudulento e transferências via PIX, o debate assume contornos semelhantes, pois o Poder Judiciário busca identificar se o golpe dependeu do acesso a dados internos da relação contratual, como número de contrato, valor exato da dívida ou dados bancários específicos, ou então se

poderia ter sido viabilizado exclusivamente por técnicas de engenharia social. Aqui, a responsabilização costuma ocorrer quando há coincidência precisa entre os dados utilizados pelo fraudador e informações restritas ao fornecedor. Situação análoga ocorre nas hipóteses de clonagem de cartão e compras não reconhecidas, em que o foco recai sobre a previsibilidade da fraude e os mecanismos de prevenção de transações atípicas. Ainda assim, a discussão permanece focada na ocorrência do evento e na imputação do prejuízo, e raramente evolui para análise das medidas implementadas.

- TJSP. 1004166-61.2023.8.26.0581. Relator: Rodolfo Pellizari. 15a Câmara de Direito Privado. Data de Julgamento: 11/02/2025. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/tj-sp/3059190918/inteiro-teor-3059190924>.

- TJSC. 5005056-39.2022.8.24.0025. Relator: Alex Heleno Santore. 8a Câmara de Direito Civil. Data de Julgamento: 08/07/2025. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/tj-sc/4208684553/inteiro-teor-4208684562>.

- TJPA. 0800457-39.2024.8.14.0051. Relatora: Shéri da Keila Pacheco Teixeira Bauer. 2a Turma Recursal Permanente dos Juizados Especiais. Data de julgamento: 12/09/2025. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/tj-pa/5015503690/inteiro-teor-5015503695>.

- TJSP. 1016433-74.2024.8.26.0114. Relator: Ademir Modesto de Souza. 7a Câmara de Direito Privado. Data de Julgamento: 23/04/2025. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/tj-sp/3533422125/inteiro-teor-3533422131>.

- TJSP. 1009116-27.2024.8.26.0566. Relator: Alexandre David Malfatti. 12a Câmara de Direito Privado. Data de Julgamento: 13/12/2024. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/tj-sp/2928052603/inteiro-teor-2928052606>.

- TJPR. 0003121-25.2022.8.16.0105. Relatora: Elizabeth de Fátima Nogueira Calmon de Passos. 10a Câmara Cível. Data de Julgamento: 18/09/2025. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/tj-pr/4939141520/inteiro-teor-4939141526>.

• TJPR. 0004696-42.2021.8.16.0028. Relator: Eugenio Achille Grandinetti. 2a Câmara Cível. Data de Julgamento: 17/02/2025. Disponível em: www.jusbrasil.com.br/jurisprudencia/tj-pr/3079739197/inteiro-teor-3079739199.

Incidente de segurança

Nos casos de incidente propriamente dito, como a invasão de conta, ataque hacker, vazamento massivo de dados e posterior circulação em fóruns ou dark web, o foco das decisões passa a ser a análise da estrutura de segurança adotada pelo agente. Aqui, o incidente costuma ser reconhecido como evento ocorrido, e a controvérsia gira em torno da existência ou não de falha imputável ao controlador. Portanto, o debate se aproxima de forma mais direta do dever de segurança do art. 46 da LGPD.

As decisões tendem a examinar, ainda que de forma pouco sistematizada, aspectos como mecanismo de autenticação, política de senha, autenticação em dois fatores, controles de acesso interno, monitoramento de atividades suspeitas, protocolo de bloqueio preventivo e resposta a incidentes. Nos casos de invasão de conta, o ponto central costuma ser a suficiência de mecanismos de autenticação. Questiona-se se a empresa adotou barreiras adequadas para impedir acessos indevidos ou se havia alguma fragilidade estrutural no sistema. Ainda assim, a análise frequentemente é genérica, com referências abstratas ao dever de proteção, sem detalhamento técnico sobre padrões mínimos esperados.

Já nos ataques hackers e vazamentos massivos, especialmente quando há alegação de exposição de bases inteiras de dados e/ou disponibilização em ambientes da dark web, o debate assume contornos mais amplos. Nesses casos, a controvérsia envolve não só o acesso indevido, mas a dimensão coletiva do incidente e o seu potencial impacto sistêmico. Mesmo assim, o foco da fundamentação costuma ser a responsabilidade civil, analisando nexos causal e dever de indenizar, e não a análise de aspectos de segurança.

Nesses casos, é frequente a invocação da tese de fortuito externo. Parte das decisões afasta a responsabilidade quando entende que o ataque decorreu de ação criminosa sofisticada e inevitável de terceiros, em especial quando não há demonstração concreta de vulnerabilidade do sistema. Outras, no entanto, adotam compreensão mais rigorosa, reconhecendo que a própria atividade de

tratamento possui riscos inerentes, portanto, ataques externos não afastam automaticamente a responsabilidade quando houver indícios de fragilidade na proteção dos dados. Mesmo aqui, a discussão permanece centrada na verificação da falha que teria permitido o acesso indevido e nonexo causal com o dano alegado pelo titular.

- TJMG. 5064103-55.2019.8.13.0024. Relator: Luiz Carlos Gomes da Mata. 13a Câmara Cível. Data de julgamento: 12/06/2025. Disponível em: <http://jusbrasil.com.br/jurisprudencia/tj-mg/4056246876/inteiro-teor-4056246886>.

- TJMG. 5053712-65.2022.8.13.0079. Relator: Amorim Siqueira. 9o Câmara Cível. Data de Julgamento: 08/10/2024. Disponível em: jusbrasil.com.br/jurisprudencia/tj-mg/2903369971/inteiro-teor-2903370024. O TJPA. 0875100-96.2021.8.14.0301. Relatora: Maria Filomena de Almeida Buarque. 1a Turma de Direito Privado. Data de Julgamento: 19/05/2025. Disponível em: <http://jusbrasil.com.br/jurisprudencia/tj-pa/3935241566>.

- TJAL. 0709098-65.2022.8.02.000. Relator: Orlando Rocha Filho. 4a Câmara Cível. Data de Julgamento: 22/01/2025. Disponível em: <http://jusbrasil.com.br/jurisprudencia/tj-al/3005846356/inteiro-teor-3005846357>.

- TJMG. 5005995-77.2024.8.13.0567. Relator: Monteiro de Castro. 15a Câmara Cível. Data de Julgamento: 15/08/2025. Disponível em: <http://jusbrasil.com.br/jurisprudencia/tj-mg/4560349299/inteiro-teor-4560349307>.

- TJPE. 0000458-51.2024.8.17.2160. Relator: Luciano de Castro Campos. 1a Turma da Câmara Regional de Caruaru. Data de Julgamento: 30/09/2025. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/tj-pe/5025730388/inteiro-teor-5025730392>.

Empréstimo consignado e benefícios previdenciários

O debate é focado na circulação e no uso de dados vinculados a benefícios concedidos pelo INSS, especialmente em contextos de crédito consignado. A controvérsia costuma envolver a licitude do acesso e uso de dados estruturais inseridos em fluxos institucionais regulares, e a demonstração do nexocausal entre o acesso indevido e o dano alegado.

O incidente é frequentemente narrado com base na coincidência temporal entre a concessão de algum benefício previdenciário e o recebimento imediato de ofertas de crédito ou mesmo a contratação não reconhecida de empréstimos. A premissa adotada pelos titulares costuma ser a de que dados como número do benefício, margem consignável ou valor disponível para a contratação não seriam acessíveis a terceiros estranhos à relação institucional, indicando possível vazamento ou compartilhamento indevido. Nesses casos, a controvérsia gira em torno da origem dos dados e da plausibilidade de que eles tenham sido obtidos a partir de base restrita. Quando não há demonstração concreta de acesso interno irregular ou qualquer falha identificável na cadeia de tratamento, a tendência dos tribunais é afastar a responsabilidade, alegando que a oferta de crédito pode decorrer de cruzamento de dados públicos, inferências mercadológicas ou práticas amplamente difundidas no setor financeiro. Já nos casos em que o terceiro demonstra conhecimento individualizado da situação previdenciária do titular, revelando informações que extrapolam dados meramente cadastrais, aumenta a possibilidade de reconhecimento de irregularidade no tratamento e imputação de responsabilidade. O nexo causal, portanto, não é presumido a partir do prejuízo experimentado, mas depende da demonstração de que as informações utilizadas no golpe estavam vinculadas, de forma específica, à base do agente demandado.

- TRF-3. 5005893-20.2024.4.03.6338. Relator: José Renato Rodrigues. 5a Turma Recursal da Seção Judiciária de São Paulo. Data de julgamento: 11/09/2025. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/trf-3/4939258419/inteiro-teor-4939258425>.

- TRF-3. 5036920-69.2023.4.03.6301. Relator: Fernando Moreira Gonçalves. 1a Turma Recursal da Seção Judiciária de São Paulo. Data de julgamento: 10/09/2025. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/trf-3/4927507378/inteiro-teor-4927507385>.

- TRF-3. 0006532-36.2021.4.03.6304. Relatora: Janaína Rodrigues Valle Gomes. 12a Turma Recursal da Seção Judiciária de São Paulo. Data de Julgamento: 16/10/2024. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/trf-3/2944783518/inteiro-teor-2944783521>.

- TRF-4. 5023469-51.2023.4.04.7205. Relator: Gilson Jacobsen. 3a Turma Recursal de Santa Catarina. Data de Julgamento: 13/02/2025. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/trf-4/3068319324/inteiro-teor-3068319334>.

- TRF-4. 5009402-80.2024.4.04.7000. Relator: Gerson Luiz Rocha. 1a Turma Recursal do Paraná. Data de Julgamento: 02/06/2025. Disponível em: jusbrasil.com.br/jurisprudencia/trf-4/3976477119/inteiro-teor-3976477126.

Essas categorias não são mutuamente exclusivas, e um mesmo precedente pode envolver múltiplas tipologias, como fraude associada à alegação de vazamento. Ainda assim, a análise revela uma tendência relevante: o incidente de segurança costuma ser judicializado predominantemente como fraude ou irregularidade individualizada, com repercussão patrimonial imediata e foco na reparação do dano concreto. Isso explica por que a jurisprudência brasileira privilegia os arts. 44 e 46 da LGPD, que são usados como fundamentos de enquadramento da irregularidade e responsabilização pelo evento consumado. Em contrapartida, os arts. 47, 48 e 49, sobre comunicação de incidentes e estrutura de governança, aparecem de forma residual. O centro da controvérsia permanece, portanto, na imputação do dano individual e nonexo causal.

Golpe do boleto falso | Condenação do agente de tratamento

Dispositivos da LGPD citados: ART. 44

Trata-se de ação proposta por empresa consumidora contra a concessionária de energia elétrica após ter sido vítima do "golpe do boleto falso". A autora relatou que recebeu, por e-mail, fatura aparentemente legítima de energia elétrica e efetuou o pagamento. Depois, foi informada de que o débito permanecia em aberto, momento em que constatou que o boleto quitado era fraudulento, o que a levou a realizar novo pagamento para evitar interrupção do serviço.

Nos autos, ficou demonstrado que um terceiro fraudador acessou indevidamente o sistema da concessionária e alterou o e-mail cadastrado da autora, passando a interceptar as comunicações oficiais. De posse de dados da unidade consumidora, histórico de consumo, endereço e CNPJ, o estelionatário conseguiu emitir e encaminhar um boleto com aparência legítima à vítima. Com base na perícia, o TJSC entendeu que o golpe só foi possível porque houve falha de segurança no sistema da empresa, que permitiu a alteração de dados cadastrais sensíveis sem mecanismos adicionais de verificação ou alerta ao titular. A ausência de medidas de segurança robustas, como a autenticação adicional ou a confirmação da alteração cadastral, evidenciou vulnerabilidade no tratamento das informações. O acórdão destacou que o acesso indevido a dados da relação de consumo e a utilização dessas informações para a elaboração do boleto fraudado configuram tratamento inadequado de dados

em afronta aos princípios e às obrigações de segurança previstos na LGPD.

Assim, entendeu-se pela responsabilidade da fornecedora. Diante disso, foi mantida a condenação da concessionária à restituição do valor pago em duplicidade, visto que a fraude decorreu de falha na segurança das informações tratadas pela empresa, que possibilitou o sucesso do golpe.

TJSC, 5005056-39.2022.8.24.0025, Relator Des. Alex Heleno Santore, Data de julgamento: 08/07/2025, 8a Câmara de Direito Civil, Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/tj-sc/4208684553/inteiro-teor-4208684562>.

Golpe do boleto falso | Culpa concorrente do titular (vítima)

Dispositivos da LGPD citados: ART. 6º, VII E VIII

Trata-se de ação proposta por consumidora contra concessionária de energia elétrica após ter sido vítima do “golpe do boleto falso”. A autora alegou que quitou duas faturas de energia elétrica por meio de boletos aparentemente legítimos, mas posteriormente notou que os débitos continuavam pendentes no sistema da empresa. Diante da ameaça de suspensão do serviço, realizou novo pagamento e ajuizou ação requerendo restituição em dobro dos valores pagos e indenização por danos morais.

No processo, ficou demonstrado que terceiros fraudadores tiveram acesso aos dados da relação contratual da consumidora, como informações da unidade consumidora, valores e consumo, utilizando essas informações para confeccionar boletos com aparência legítima e direcionar o pagamento a terceiros. O TJPA reconheceu que a fraude decorreu de falha na segurança das informações tratadas pela concessionária, que permitiu o uso indevido de dados da consumidora, caracterizando violação aos princípios da segurança e da prevenção previstos na LGPD.

No entanto, o acórdão identificou culpa concorrente da consumidora, uma vez que ela não verificou o destinatário do pagamento antes de confirmar a operação. Dessa maneira, embora tenha sido reconhecida a falha de segurança no tratamento de dados, entendeu-se que a falta de cautela da consumidora contribuiu para a concretização da fraude. Diante disso, o TJPA afastou a condenação por danos morais e a restituição em dobro, mantendo tão somente a restituição simples dos valores pagos indevidamente, já impostos em sentença.

TJPA, 0800457-39.2024.8.14.0051, Relator Juíza Shériida Keila Pacheco Teixeira Bauer, Data de julgamento: 12/09/2025, 2a Turma Recursal Permanente dos Juizados Especiais, Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/tj-pa/5015503690/inteiro-teor-5015503695>.

Dados previdenciários e ofertas de crédito | Inexistência de vazamento

Dispositivos da LGPD citados: ARTS. 1º, 7, I E § 5º, 21, 26, CAPUT E § 1º, 27, 42, 44 E 46.

Trata-se de ação indenizatória proposta por beneficiária do INSS em face do INSS e da DATAPREV, sob a alegação de que teria havido vazamento dos seus dados pessoais previdenciários, o que teria possibilitado a realização de descontos consignados fraudulentos e recebimento insistente de ofertas de crédito através de ligações e mensagens. A autora sustentou violação à LGPD e requereu indenização por danos morais.

Em primeiro grau, os réus foram condenados solidariamente ao pagamento de indenização, sob o fundamento de que teriam falhado no dever de guarda, sigilo e proteção dos dados da segurada. Contudo, ao julgar o recurso, o TRF-3 reformou a sentença. O colegiado entendeu que, quanto ao INSS, não ficou configurada a sua legitimidade para responder civilmente pelo suposto vazamento de dados, considerando que os dados do benefício, após a concessão, são geridos, tratados e operacionalizados pela DATAPREV.

Além disso, no tocante aos descontos consignados fraudulentos, o TRF-3 destacou que a controvérsia já vinha sendo discutida em ações próprias contra as instituições financeiras e associações envolvidas, não sendo possível imputar automaticamente ao INSS a responsabilidade pretendida. Em relação à DATAPREV, o acórdão concluiu que, embora a narrativa da autora apresentasse plausibilidade, não houve comprovação suficiente do nexo causal entre eventual falha no tratamento de dados e os contatos promocionais ou fraudes relatadas.

O TRF-3 ressaltou que o simples fato de a autora passar a receber ofertas de crédito não permite presumir, por si só, que tenha ocorrido vazamento imputável à empresa pública. As abordagens insistentes de instituições financeiras, no caso, não foram consideradas para fins de dano moral indenizável.

Assinalou-se ainda que eventual responsabilidade pelas ofertas abusivas deveria ser buscada em ação própria contra as instituições financeiras responsáveis pelos contatos. Diante disso, o recurso foi provido para extinguir sem resolução de mérito os pedidos formulados contra o INSS quanto ao alega

do vazamento de dados e julgar improcedentes os demais pedidos, inclusive em relação à DATAPREV.

TRF-3, 5005893-20.2024.4.03.6338, Relator Juiz José Renato Rodrigues, Data de julgamento: 11/09/2025, 5ª Turma Recursal da Seção Judiciária de São Paulo, Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/trf-3/4939258419/inteiro-teor-4939258425>.

Dados previdenciários e ofertas de crédito | Condenação do INSS

Dispositivos da LGPD citados: ART. 26, § 1º

Trata-se de ação indenizatória proposta contra o INSS em razão de suposto vazamento de dados pessoais relacionados a pedido administrativo de salário-maternidade. A autora alegou que, após o indeferimento do benefício, passou a receber mensagens com oferta de consultoria previdenciária, inclusive com menção expressa ao seu processo administrativo, o que demonstraria acesso indevido a informações protegidas sob custódia da autarquia. O TRF-3 entendeu que o requerimento de salário-maternidade constitui dado sensível, por envolver informações relativas à saúde e à situação financeira da titular, atraindo proteção reforçada à luz da LGPD. No caso concreto, o TRF-3 considerou relevante o fato de a abordagem comercial ter feito referência específica ao indeferimento do pedido administrativo da autora, informação que se encontrava sob a custódia do INSS. Para o colegiado, esse contexto evidenciou o descumprimento do dever de diligência na guarda e proteção dos dados pessoais, sendo insuficiente a alegação genérica da autarquia de que haveria “complexa cadeia de transferência de dados” ou de que também seria vítima do incidente.

O acórdão destacou ainda que, na condição de agente de tratamento, incumbia ao INSS demonstrar a adoção de medidas eficazes de segurança e governança aptas a comprovar a observância das normas de proteção de dados, o que não ocorreu. Com isso, reconheceu-se a incidência da responsabilidade civil estatal e da responsabilidade prevista na LGPD. O acórdão também ressaltou o entendimento do STJ segundo o qual o vazamento de dados pessoais sensíveis pode configurar dano moral presumido, dispensando prova específica do prejuízo extrapatrimonial.

Assim, concluiu-se que a importunação sofrida pela autora, decorrente do uso indevido de dados vinculados ao pedido de salário-maternidade, ultrapassou o mero aborrecimento cotidiano, condenando-se a ré em danos materiais e morais.

TRF-3, 5036920-69.2023.4.03.6301, Relator Juiz Fernando Moreira Gonçalves, Data de julgamento: 10/09/2025, 1ª Turma Recursal da Seção Judiciária de São Paulo, Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/trf-3/4927507378/inteiro-teor-4927507385>.

Invasão de conta de rede social | Reconhecimento de falha de segurança na plataforma

Dispositivos da LGPD citados: ARTS. 44 E 46

Trata-se de ação indenizatória proposta por usuária do Instagram/Facebook após a invasão de sua conta por terceiros, que passaram a utilizar suas imagens e seu perfil para a prática de fraudes contra seguidores, com publicações enganosas voltadas à obtenção de vantagens financeiras indevidas. A autora alegou que, mesmo após comunicar administrativamente a plataforma sobre a invasão, não obteve solução efetiva em tempo hábil, permanecendo impossibilitada de retomar o controle da conta e de remover o conteúdo fraudulento.

O bloqueio do perfil somente ocorreu após determinação judicial. O TJMG entendeu que a invasão de conta em rede social configura fortuito interno, por se tratar de risco inerente à atividade desenvolvida pelo provedor da aplicação. Assim, a alegação de culpa exclusiva de terceiro não foi suficiente para afastar a responsabilidade da plataforma, uma vez que compete ao fornecedor adotar medidas adequadas para garantir a segurança das contas e dos dados dos usuários. O acórdão também destacou que a LGPD, em harmonia com o art. 14 do CDC, exige que o tratamento de dados pessoais ofereça a segurança que o titular legitimamente espera, sendo irregular o tratamento que não observe padrões adequados de proteção. Nessa linha, o TJMG consignou que a plataforma não demonstrou concretamente como ocorreu a invasão nem comprovou violação específica das práticas de segurança pela usuária, ônus probatório que lhe incumbia, dada sua posição de controladora das informações e da infraestrutura da rede social. Além da invasão em si, o TJMG considerou relevante a omissão da plataforma em solucionar administrativamente o problema, mesmo após ciência da utilização criminosa do perfil. A demora no

restabelecimento do acesso e na contenção do uso indevido da conta agravou a falha na prestação do serviço.

Diante desse contexto, o TJMG concluiu pela configuração de dano moral indenizável, destacando que a autora (à época, menor de idade) teve a sua imagem e reputação expostas em contexto de fraude praticada perante seus próprios seguidores. Por isso, foi mantida a condenação da plataforma ao pagamento de R\$ 10.000,00 por danos morais e ao bloqueio do perfil invadido.

TJMG, 5053712-65.2022.8.13.0079, Relator Des. Amorim Siqueira, Data de julgamento: 08/10/2024, 9ª Câmara Cível, Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/tj-mg/2903369971/inteiro-teor-2903370024>.

Vazamento de dados na dark web | Comprovação insuficiente

Dispositivos da LGPD citados: ARTS. 6º, 7º E 42

Trata-se de ação de indenização por danos morais proposta em face da Serasa, na qual o autor alegou ter sido vítima de vazamento de dados no contexto de incidente massivo de exposição de informações ocorrido em 2021. Sustentou que seus dados estariam circulando na dark web e que a empresa ré deveria ser responsabilizada com base na LGPD e CDC.

O TJPE manteve a sentença de improcedência por entender que não houve comprovação técnica idônea de que os dados do autor tenham sido efetivamente vazados por ação ou omissão da ré. O acórdão observou que os elementos juntados aos autos indicavam alegações genéricas e indiretas, sem demonstração concreta de que a origem da exposição estivesse vinculada aos sistemas da Serasa. A decisão também afastou a tese de dano moral presumido, destacando o entendimento do STJ no sentido de que o vazamento de dados comuns, por si só, não gera automaticamente direito à indenização. Para a configuração da responsabilidade civil, seria necessária a prova de dano moral concreto e do nexu causal entre a conduta imputada à empresa e o prejuízo alegado pelo titular dos dados. No caso, o TJPE ressaltou que não há prova de utilização fraudulenta da identidade do autor, movimentações financeiras indevidas, inscrição irregular em cadastros restritivos ou outro evento concreto capaz de evidenciar violação relevante à esfera moral do autor. A mera alegação de insegurança ou abalo psicológico genérico foi considerada insuficiente para sustentar a reparação pretendida. O acórdão consignou que relatórios de monitoramento da dark web, pareceres e documen-

tos produzidos em outros procedimentos ou ações coletivas não possuem, por si sós, força bastante para comprovar o fato constitutivo do direito em ação individual, sem demonstração específica de aplicabilidade ao caso concreto.

Diante disso, o TJPE concluiu pela ausência dos pressupostos da responsabilidade civil, especialmente da prova da conduta ilícita, do dano e do nexu causal, e negou provimento ao recurso, mantendo a improcedência dos pedidos indenizatórios.

TJPE, 0000458-51.2024.8.17.2160, Relator Des. Luciano de Castro Campos, Data de julgamento: 30/09/2025, 1ª Turma da Câmara Regional de Caruaru, Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/tj-pe/5025730388/inteiro-teor-5025730392>.

PAINEL LGPD NOS TRIBUNAIS

5

Considerações Finais

5. Considerações Finais

A presente edição do Painel LGPD nos Tribunais, que celebra cinco anos de monitoramento sistemático das decisões dos tribunais brasileiros em matéria de proteção de dados pessoais, oferece um panorama da maturidade que o Poder Judiciário vem alcançando na interpretação e na aplicação da Lei nº 13.709/2018 (LGPD).

Com a análise qualitativa de 5.555 decisões judiciais de alta relevância — selecionadas de um universo de 24.634 documentos coletados entre outubro de 2024 e outubro de 2025, recorde de todas as edições —, o Relatório ratifica tendências identificadas em ciclos anteriores e, ao mesmo tempo, revela padrões interpretativos mais densos e articulados, que sinalizam um novo patamar de consolidação da proteção de dados no contencioso brasileiro.

O universo de 24.634 documentos coletados, 55% superior ao da edição anterior, atesta o crescente peso da LGPD no cotidiano judicial, seja no enfrentamento de casos concretos, seja pela incorporação de precedentes dos tribunais superiores à fundamentação de decisões de primeira e segunda instâncias. Embora, em quantidade, as decisões versem majoritariamente sobre determinados grupos de agentes econômicos, observou-se aplicação da lei em setores variados, incluindo o poder público. O mapeamento das menções aos ramos do direito busca também demonstrar o diálogo da LGPD com múltiplos contextos normativos — do direito do consumidor ao direito do trabalho, do direito constitucional ao direito civil.

Apresentam-se, a seguir, as conclusões mais relevantes desta edição, organizadas em cinco eixos temáticos.

a. Responsabilidade civil como principal tema da jurisprudência

A responsabilidade civil permanece como o tema de maior incidência nas decisões analisadas, alcançando 2.179 casos (cerca de 39% do total). Os arts. 42 e 44 da LGPD consolidam-se como os dispositivos centrais da fundamentação jurídica empregada pelos tribunais: o art. 42 opera como cláusula geral de imputação da obrigação de reparar os danos decorrentes do tratamento irregular, enquanto o art. 44 fundamenta o enquadramento da irregularidade a partir da constatação de determinados eventos danosos. A articulação entre esses dispositivos e o art. 14 do CDC evidencia a consolidação de um modelo de responsabilidade que conjuga, de forma coordenada, os regimes da LGPD e do direito do consumidor.

Nesse contexto, o REsp 2.077.278/SP (STJ, Terceira Turma, rel. min. Nancy Andrighi, 2023) figura entre os precedentes mais citados no período. Com fundamento no art. 43 da LGPD e na Súmula 479 do STJ, o acórdão consolidou a responsabilidade objetiva de instituições financeiras pelo tratamento inadequado de dados bancários sigilosos que permitem ou facilitam atividade fraudulenta em prejuízo do consumidor — reforçando o entendimento de que a falha no tratamento de dados pode configurar defeito na prestação do serviço, independentemente da participação de terceiros.

b. Incidentes de segurança e princípios da segurança e prevenção

A discussão sobre incidentes de segurança é uma das tendências mais persistentes ao longo das cinco edições do Painel. Os casos envolvem, principalmente, golpes e fraudes financeiras praticadas contra consumidores, invasões de contas em redes sociais e celebração ou alteração de contratos por terceiros em nome do titular dos dados.

Para além dos dispositivos de responsabilidade, as decisões recorrem com frequência crescente aos princípios da segurança e da prevenção (art. 6º da LGPD) e ao art. 46 da LGPD, ressaltando o dever de adoção de medidas técnicas e administrativas adequadas à proteção dos dados tratados. Nota-se, porém, que grande parte dessas decisões não especifica quais iniciativas concretas deveriam ter sido implementadas pelo agente de trata-

mento — lacuna que revela, ao mesmo tempo, uma limitação da argumentação judicial e uma oportunidade para o desenvolvimento de parâmetros técnico-normativos mais precisos.

c. Base Legal da proteção ao crédito e ciclo da vida dos dados

A proteção ao crédito (art. 7º, X, da LGPD) destaca-se como a base legal com maior incidência setorial nesta edição, com especial concentração nos casos envolvendo gestores de bancos de dados de cadastro e consumidores. Dois principais debates orientam os casos analisados.

O primeiro refere-se à manutenção de dados de dívida prescrita em plataformas de negociação. Submetida ao STJ por meio do Tema Repetitivo n. 1.264 e objeto de IRDR no TJMG, a questão examina a transição entre as bases legais da proteção ao crédito e do consentimento quando a dívida prescreve e o dado permanece no cadastro do titular, colocando em evidência o debate sobre o ciclo de vida dos dados pessoais no sistema creditício.

O segundo debate diz respeito à conduta de gestores de bancos de dados que disponibilizam dados pessoais de titulares a terceiros consulentes. A Terceira Turma do STJ tem entendido, por maioria, que a base legal da proteção ao crédito não autoriza esse compartilhamento amplo: nesses casos, a Corte afirma ser necessário o consentimento específico do titular (art. 7º, I), em articulação com a Lei n. 12.414/2011. Parcela dos ministros da Turma, no entanto, sustenta que o inciso X alcança igualmente essas situações, demonstrando que o debate ainda não está encerrado.

d. Direito dos titulares e decisões automatizadas

Das 5.555 decisões analisadas, 2.107 (38%) abordam direitos dos titulares. O direito à revisão de decisões automatizadas (art. 20 da LGPD) é o dispositivo mais explicitamente invocado nesse conjunto, sendo utilizado como fundamento para exigir transparência sobre os critérios da decisão automatizada, explicação das razões do bloqueio de perfil e garantia de revisão humana das decisões de plataformas.

Na Justiça do Trabalho, o art. 20 é articulado com normas trabalhistas para questionar a licitude do bloqueio ou da suspensão automatizada de contas de motoristas e entregadores de aplicativos. A jurisprudência ainda oscila, uma vez que parte das decisões reconhece a ilicitude do bloqueio sem possibilidade de defesa ou revisão humana, determinando o pagamento de danos morais e a reativação da conta; outra parte exige a comprovação de pedido prévio de revisão pelo titular como condição para eventual responsabilização do agente de tratamento.

e. Categorização do dado pessoal e dado pessoal sensível para fins de reconhecimento de dano presumido

A distinção entre dado pessoal não sensível e dado pessoal sensível (art. 5º, I e II, da LGPD) permanece como um dos eixos de maior debate na jurisprudência sobre proteção de dados. O debate foi inaugurado, no âmbito do STJ, pelo AREsp 2.130.619/SP (Segunda Turma, rel. min. Francisco Falcão, 2023), que afastou a presunção de dano moral em casos envolvendo dados pessoais não sensíveis, exigindo a comprovação de prejuízo concreto.

Esse entendimento foi progressivamente tensionado pela Terceira Turma, que, ao julgar os REsp 2.133.261/SP e REsp 2.115.461/SP (outubro de 2024, rel. min. Nancy Andrighi, Informativo n. 833), consignou que a disponibilização indevida de dados pessoais por gestores de bancos de dados a terceiros consulentes — em desacordo com a Lei n. 12.414/2011 — é apta a gerar dano moral presumido (*in re ipsa*), independentemente de prova de prejuízo concreto. Em 2025, o REsp 2.201.694/SP, também relatado pela ministra Andrighi, reconheceu o dano moral presumido com fundamento na violação à autodeterminação informativa como bem jurídico autônomo, tutelado pela LGPD e pela Emenda Constitucional n. 115/2022.

Esse posicionamento, no entanto, não foi o mesmo adotado na Quarta Turma, que, em novembro de 2025, ao julgar o REsp 2.221.650/SP sob a relatoria da ministra Isabel Gallotti, entendeu que seria exigida a demonstração de abalo significativo aos direitos da personalidade para fins de indenização.

Com a sistematização, neste Relatório, dos achados mais relevantes extraídos da análise das decisões proferidas pelo Poder Judiciário, encerra-se esta 5ª edição do estudo, na expectativa de contribuir para os rumos da proteção de dados pessoais no Brasil, seja na orientação de eventuais proposituras normativas e o adensamento da fundamentação das decisões judiciais, seja no fomento de iniciativas acadêmicas voltadas à consolidação da LGPD e do sistema de proteção de dados pessoais.