



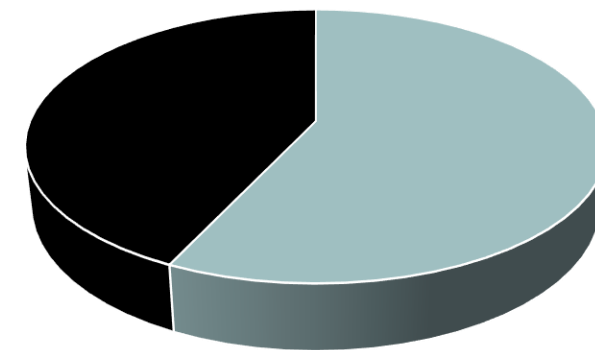


# LGPD nos Tribunais

Identificando tendências por meio de uma análise das decisões dos principais tribunais do país.

Parâmetros:

- (a) Tribunais Estaduais de 09 estados
- (b) Período de 01 ano (01/10/22 a 01/10/23)
- (c) Análise de 1.234 decisões consideradas relevantes\*



■ Outros (57%) ■ TJSP (43%)

\* Decisões em que a LGPD é a questão central do caso ou, mesmo sendo incidental, foi abordada de forma relevante.

# Take-Aways

1 Setores Envolvidos

2 Áreas do Direito

3 Princípios Aplicados

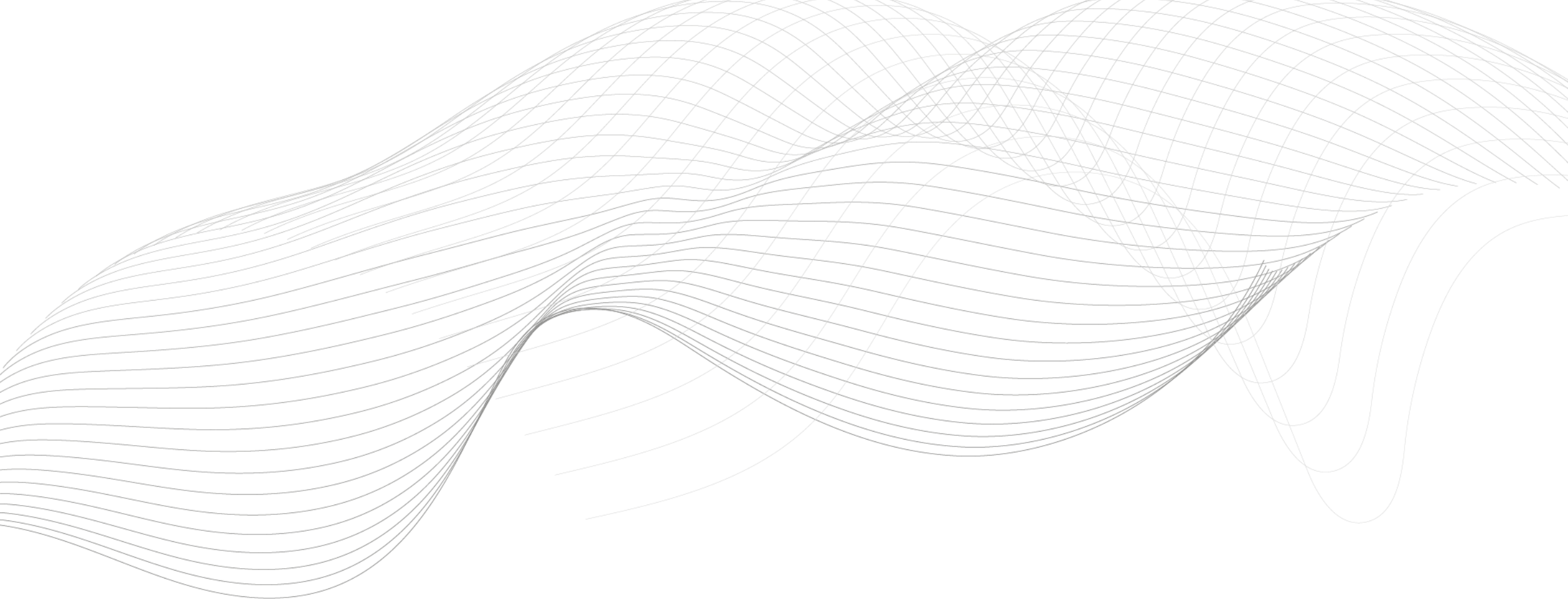
4 Artigos Mencionados

5 Bases Legais

6 Direitos dos Titulares

7 Responsabilidade Civil

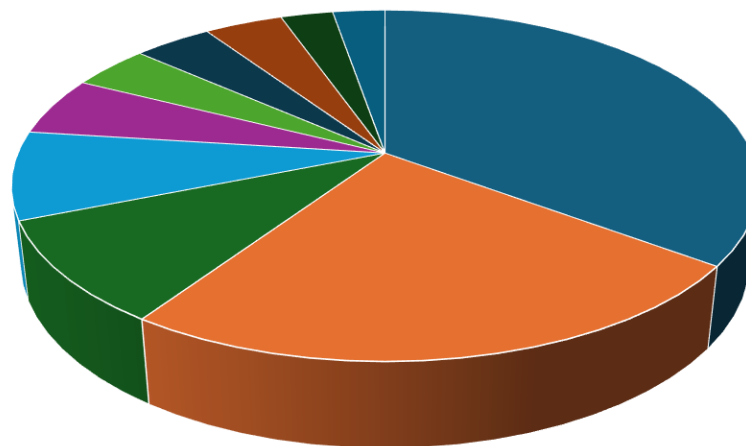
8 Conclusões



# Setores Envolvidos

# Setores Envolvidos

Setores



- |                    |                               |
|--------------------|-------------------------------|
| ■ Financeiro (26%) | ■ Banco de Dados (18%)        |
| ■ Telecom (7%)     | ■ Recuperação de Crédito (6%) |
| ■ Serviços (4%)    | ■ Transportes (3%)            |
| ■ Internet (3%)    | ■ Médico (3%)                 |
| ■ Eletrônicos (2%) | ■ Varejo (2%)                 |

### Dispositivos da LGPD citados: Art. 6º, VII e VIII.

A decisão analisa três recursos interpostos por um titular, uma instituição financeira e uma empresa do ramo de telecomunicações, em razão de “excessivas ligações, em dias e horários inoportunos” ao titular e a “seus parentes para fins de cobrança de dívida”. A decisão recorrida condenou as duas empresas solidariamente por danos morais, determinando, à empresa de telecomunicações, a se abster “de compartilhar os dados vinculados aos dependentes da [titular] em seu plano familiar sem a sua autorização ou ordem judicial”, e, à empresa do ramo financeiro, a excluir “do seu cadastro os números de telefones vinculados aos dependentes da autora”. Ao analisar os recursos, O Tribunal entendeu pela manutenção do dever de indenização por dano moral das duas instituições. Por maioria, verificou-se a prática de ato ilícito da empresa de telecomunicações, que não “comprovou especificamente a maneira pela qual conseguiu os números de telefone do marido e do filho da parte autora”, de modo que não “zelou pela proteção dos dados da consumidora”, conforme Art. 6º, VII e VIII, da LGPD. Assim, (i) a empresa de telecomunicações foi condenada a responder objetivamente pelos danos causados, de acordo com o Art. 14 do CDC, e (ii) a instituição financeira foi condenada a excluir, do seu cadastro, o número de telefone da titular.

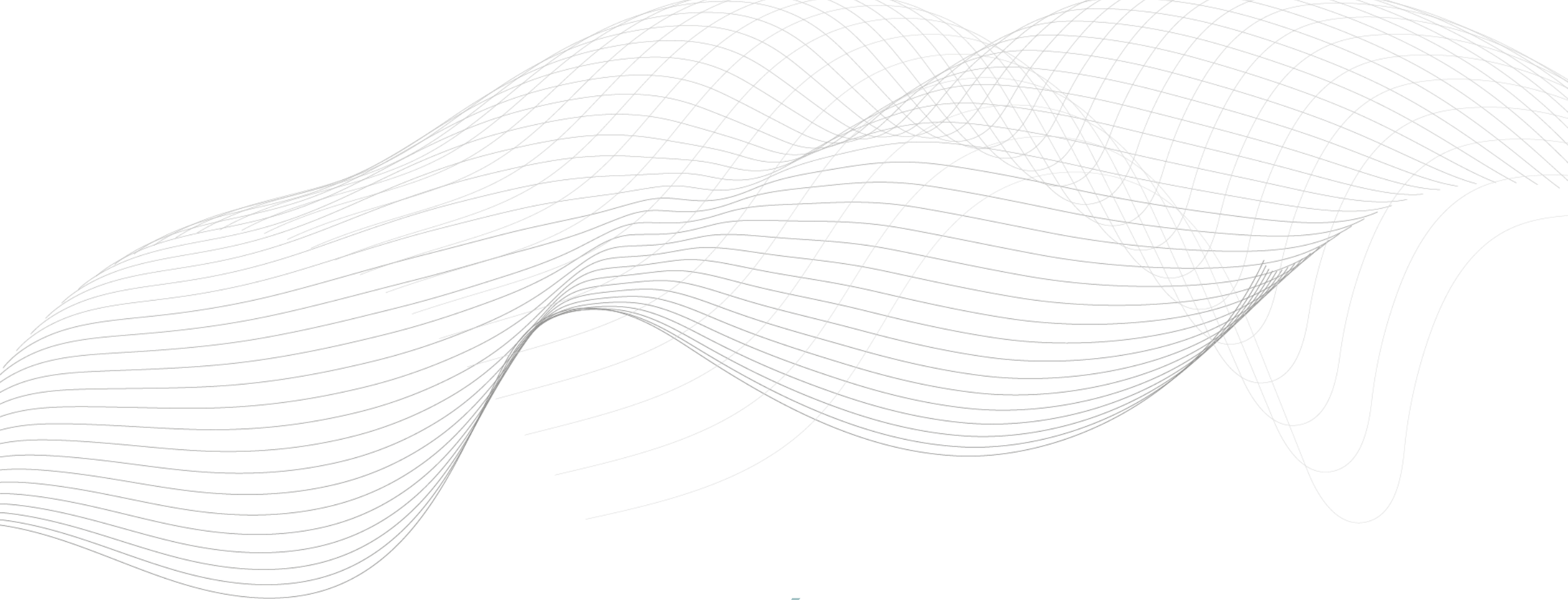
TJDFT - Recurso Inominado Cível nº 0726222-75.2022.8.07.0016, Juiz: Antonio Fernandes da Luz, 1ª Turma Recursal do Tribunal de Justiça do Distrito Federal e dos Territórios/DF, Data de Julgamento: 19/05/2023. Disponível em: <http://www.jusbrasil.com.br/jurisprudencia/1852794259>.

### Dispositivos da LGPD citados: Art. 5º, II.

A decisão avalia as alegações de um titular de dados contra uma instituição do ramo financeiro sobre a suposta divulgação indevida de seus dados telefônicos, que teriam sido **incluídos na plataforma da empresa sem que tivessem relação com o risco de crédito e ainda sem o seu consentimento**, em violação ao Art. 43, §2º, da LGPD. Considerou-se que os dados mantidos pela empresa com relação à titular (“como nome da mãe, número de CPF, data de nascimento, grau de escolaridade, endereço, telefones e renda presumida”) **não são considerados sensíveis**, nos termos do Art. 5º, II, da LGPD, e do artigo 3º § 3º, II da Lei nº 12.414/11 (Lei do Cadastro Positivo). Entendeu-se que a **atividade comercial da empresa no uso de tais dados é para a “avaliação da situação econômica e do risco do consumidor perante o mercado de consumo”, atividade lícita**, conforme definido no julgamento do REsp nº 1.419.697/RS (Tema nº 710) e na Súmula STJ nº 550. Ademais, **as informações não foram consideradas sensíveis ou excessivas** e, por não se identificar a “recusa injustificada de crédito por uso de dados incorretos ou desatualizados da consumidora”, compreendeu-se que não houve prática de “ato ilícito” por parte da empresa capaz de justificar a exclusão dos registros ou condená-la por danos morais.

TJSP - Apelação Cível nº 1001195-33.2022.8.26.0648, Relator (Desembargador): Arantes Theodoro, 36ª Câmara de Direito Privado de São Paulo/SP, Data de Julgamento: 13/12/2022. Disponível em: <http://www.jusbrasil.com.br/jurisprudencia/1723695539>.



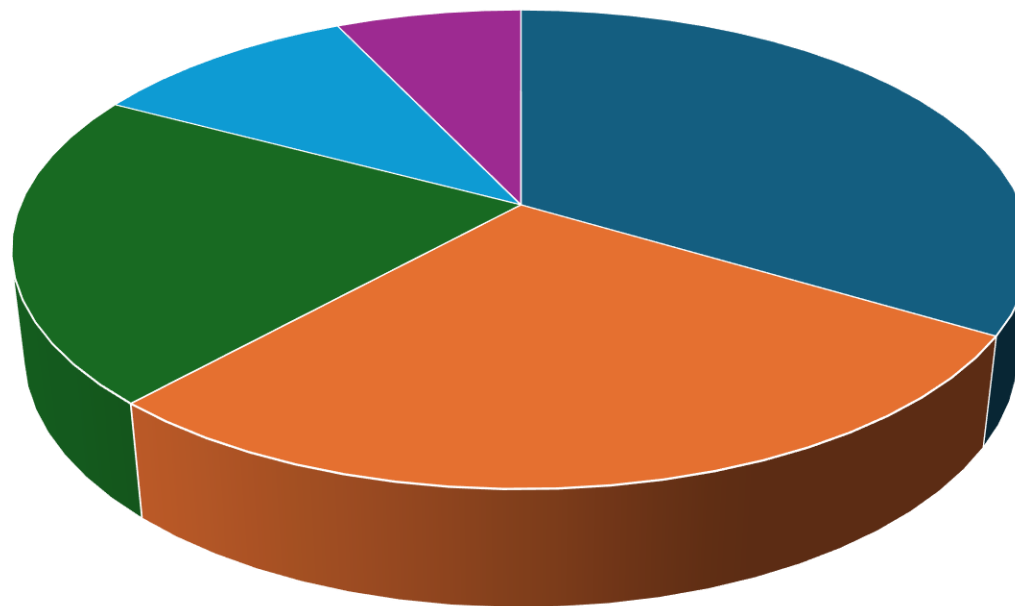


# Áreas do Direito



# Áreas do Direito

Área do Direito



■ Consumidor (43%) ■ Trabalho (36%) ■ Civil (27%)  
■ Processo (13%) ■ Constitucional (9%)

### Dispositivos da LGPD citados: Art. 42 e Art. 46.

Trata-se de caso relacionado ao pagamento de boleto falso a partir de fraude cometida por terceiro que detinha informações do consumidor prejudicado. Segundo o TJPR, se os dados que o estelionatário detinha foram obtidos em decorrência da omissão da instituição financeira em adotar as medidas de segurança necessárias de proteção de dados, sua responsabilidade é inerente ao contrato firmado com o consumidor. A conduta da instituição financeira resultou, assim, não somente na violação dos dados, mas em danos materiais e morais ao consumidor (titular dos dados). Dessa forma, o TJPR concluiu que a instituição financeira possui um dever contratual implícito de proteção e tratamento adequado dos dados do consumidor. Essa obrigação legal decorre da legislação consumerista e da LGPD, mais especificamente do seu Art. 46.

TJPR – Ap. Cív. nº 0009331-38.2022.8.16.0026, Des. Rel. Rogério Luis Nielsen Kanayama, Data de Julgamento: 05/09/2023. Disponível em: <http://www.jusbrasil.com.br/jurisprudencia/1959429706>.



### Dispositivos da LGPD citados: Art. 1º; Art. 2º.

O caso versa sobre mandado de segurança impetrado por empregado em face de decisão que autorizou o fornecimento irrestrito de dados de geolocalização do empregado, sem ressalva de horário, em fins de semana ou em feriados. A autorização havia sido solicitada pelo empregador num processo trabalhista para que se verificasse a regularidade da jornada de trabalho realizada pelo empregado. O empregado alega que a decisão viola seu direito à privacidade e à inviolabilidade das comunicações, previstos nos incisos X e XII do Art. 5º da Constituição Federal, além de outras normas internacionais. O Tribunal reconheceu que a decisão violava esse direito fundamental, além de violar a própria LGPD. Isso porque, considerando a LGPD, o direito à privacidade deveria ser considerado em sentido amplo, o que incluiria os dados de localização diante de sua liberdade de ir e vir. Dessa forma, a empresa empregadora não pode coletar informações de geolocalização do empregado para que fosse analisado como prova em processo trabalhista.

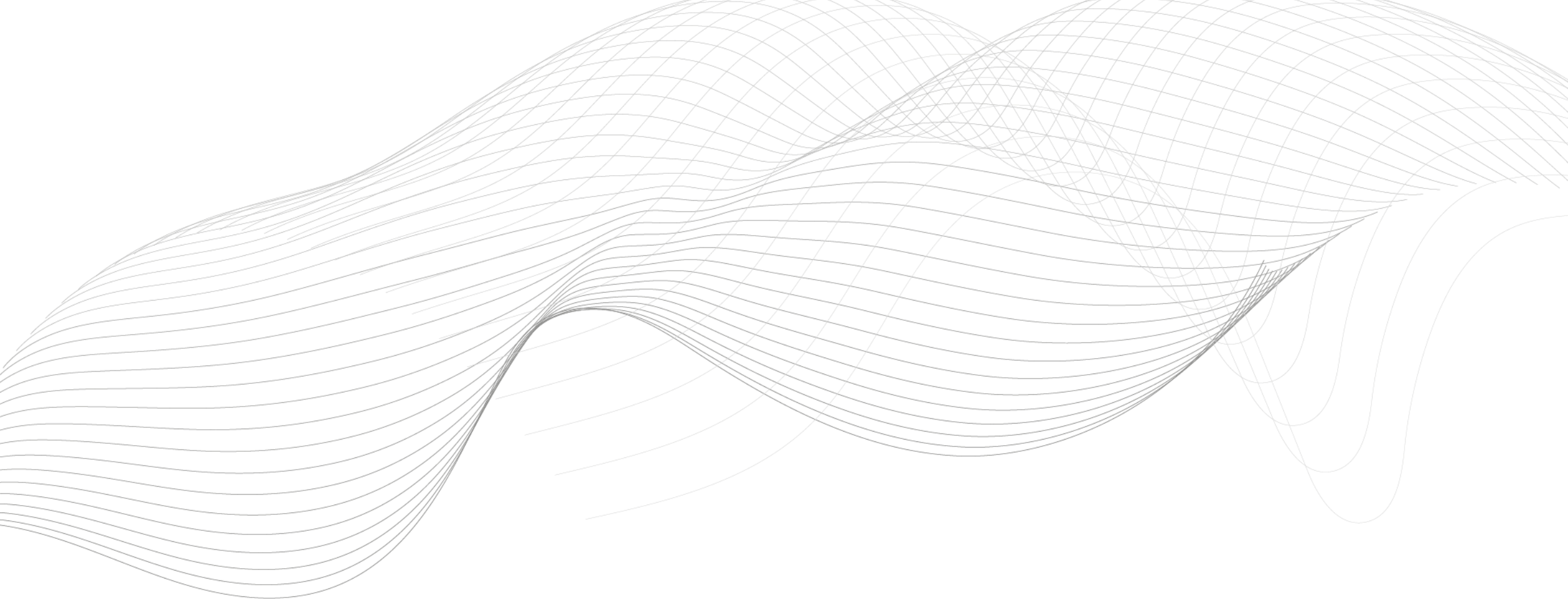
TRT4ª Região, Mandado de Segurança nº 0023218-21.2023.5.04.0000, Min. Rel. Marcelo José Ferlin, 24/04/2023. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/trt-4/1820584649/inteiro-teor-1820584653>.

**Dispositivos da LGPD citados: Art. 5º, VI e VII; Art. 6º, VII e VIII; Art. 7º; Art. 46; Art. 50.**

Ação reclusória trabalhista ajuizada por titular contra empresa do ramo de laticínios. Dentre os argumentos em debate, a titular solicitou a reversão da extinção contratual por falta grave para dispensa sem justa causa após ela ter **divulgado a todos os empregados planilha com dados funcionais de todos os colaboradores via e-mail**. Essa circunstância implicou em publicização ampla de dados, envolvendo seus endereços, documentos pessoais, salários e benefícios auferidos". Na decisão, reconheceu-se a "gravidade da exteriorização de dados pessoais estruturados pela reclamada, por absoluta falta de consentimento dos seus titulares e pela violação dos princípios da finalidade, adequação e necessidade", dispostos na LGPD. **Verificou-se, ainda, que a própria empresa violou a LGPD por não implementar medidas técnicas e administrativas para a prevenção "de danos em virtude do tratamento de dados pessoais", já que não "havia distinção no acesso aos dados funcionais". Constatou-se a "inexistência de política e governança de controle de informações", de modo que o erro da funcionária "inseriu-se em um panorama de flagrante descontrolo protetivo de dados". Assim, entendeu-se que o titular não poderia sofrer a penalidade máxima, e o pedido de reversão da justa causa foi acolhido. Na decisão, verificou-se a desproporcionalidade da medida contra o titular e a violação ao princípio da isonomia, pois não houve sanção ao empregado "responsável pela transposição de dados aos quais sequer deveria ter o acesso confiado". Ademais, houve recomendação à empresa para adoção de "providências materiais e efetivas voltadas à tutela de dados pessoais armazenados em banco de dados, como já orientam os artigos 46 e 50 da LGPD".**

TRT9 - Ação Reclusória Trabalhista nº 0000206-09.2023.5.09.0656, Juiz: Roberto Wengrzynowski, Vara do Trabalho de Castro/PR Data de Julgamento: 09/08/2023. Disponível em: <http://www.jusbrasil.com.br/jurisprudencia/1927910905>.

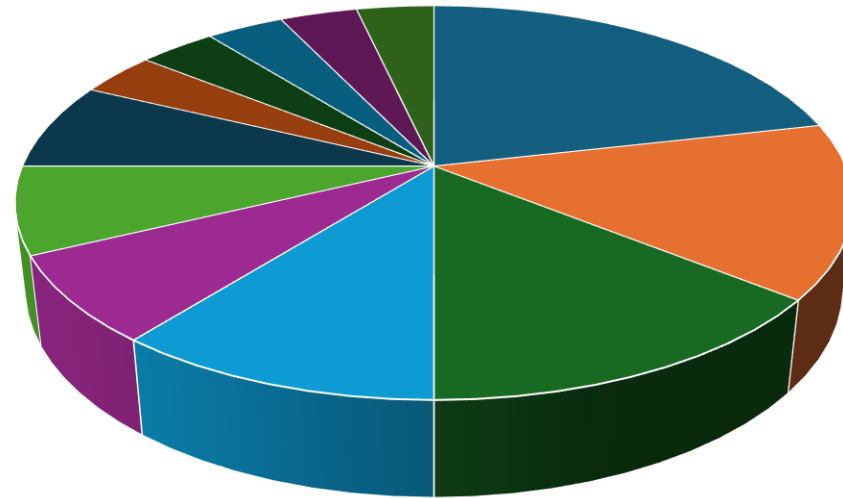




# Princípios Aplicados

# Princípios Aplicados

Princípios (Art. 6º)



- Não Discriminação (6%)
- Segurança (4%)
- Boa fé (4%)
- Finalidade (3%)
- Adequação (2%)
- Necessidade (2%)
- Prevenção (2%)
- Livre Acesso (1%)
- Qualidade dos Dados (1%)
- Transparência (1%)
- Responsabilidade (1%)
- Prestação de Contas (1%)

# Princípios Aplicados

## Princípio da Transparência

**Dispositivos da LGPD citados: Art.6º, IV; Art. 2º, II.**

Trata-se de recurso ordinário interposto para reversão de justa causa, pois a autora alega que tal penalidade foi aplicada em virtude de **prova ilícita obtida a partir da quebra do seu sigilo de correspondência telemática**, sem qualquer autorização, sendo assim ilegal. Neste caso, o aplicativo de comunicação acessado pela autora (**WhatsApp**) é de uso particular e, apesar de realizada através do celular corporativo, **não há prova de que ela foi devidamente notificada previamente da destinação exclusiva do WhatsApp do celular corporativo para as atividades profissionais e de que tais comunicações estariam sujeitas a monitoramento e gravação, com amplo acesso pela empresa empregadora**. O TRT-3 sinalizou que a cientificação prévia do trabalhador sobre o possível monitoramento e gravação das conversas em celular corporativo não configura obstáculo ao direito à ampla defesa, mas adimplemento do dever de lealdade e boa-fé. Assim, reconheceu que o **princípio da transparência (Art. 6º, VI) não foi observado pela empresa, porque, apesar de o termo de compromisso assinado pela autora constar que o uso do celular corporativo se restringia a fins profissionais, não há a informação clara e expressa de que a integralidade das comunicações realizadas por intermédio dele estariam sujeitas a monitoramento e gravação, com amplo acesso pela empregadora**. O acesso da empresa às conversas de WhatsApp particulares e íntimas da autora com o ex-empregado, sem que ela tivesse sido informada e consentido previamente quanto à possibilidade, no entendimento do TRT-3, extrapola os limites do poder empregatício e da boa-fé objetiva, ofendendo os direitos fundamentais à intimidade, privacidade e proteção dos dados pessoais. Ainda, a utilização de conversas mantidas diretamente pela autora com terceiros não encontra qualquer amparo na jurisprudência dos Tribunais Superiores, pois é pacífico no TST e no STF que a admissão de gravações feitas sem o conhecimento de uma das partes exige que o responsável pela coleta da conversa seja um dos seus interlocutores.

TRT3 – ROT nº 0010305-08.2022.5.03.0020, Rel. Des. Marcelo Lamego Pertence, Data de julgamento: 06/09/2023. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/trt-3/1962090969/inteiro-teor-1962090972>.



# Princípios Aplicados

Princípio do Livre Acesso

**Dispositivos da LGPD citados: Art. 5º, V; Art. 6º, IV; Art. 7º, VI.**

No caso, o sindicato autor apresentou pedido para que a empresa apresentasse a declaração do CAGED e/ou e-Social para verificar quais trabalhadores que já saíram deveriam receber o vale alimentação. A ré defendeu a ausência de interesse processual, porquanto o sindicato não indicou nenhum trabalhador, tampouco apresentou qualquer fundamentação legal para o pedido que impunha a ela a obrigação de exibir documentos dos funcionários, defendendo a existência de suposta vedação legal para o pedido em virtude da LGPD, que “impede que a recorrente forneça de modo indiscriminado e sem prévio conhecimento e anuência informações pessoais dos seus funcionários.” O TRT-23 concluiu que o sindicato apresentou justo motivo para a exibição dos documentos, pois, apesar de ter ajuizado ação de produção antecipada de provas, a ré não juntou nenhum documento, razão pela qual o sindicato se viu obrigado a ingressar com a nova ação, a fim de instruir o processo para condenar a empresa ao pagamento de cestas básicas durante toda a obrigatoriedade das convenções coletivas. **Ainda, entendeu que a LGPD não constitui óbice para exibição dos documentos, pois os empregados são os titulares dos dados dispostos nos documentos contratuais trabalhistas mantidos pela empresa, detendo a garantia legal de acesso a eles, de forma facilitada, mesmo que finalizado o vínculo trabalhista, conforme o princípio do livre acesso (Art. 6º, IV, da LGPD).**

TRT23 – ROT nº 0000746-05.2022.5.23.0009, Rel. Des. Eleonora Alves Lacerda, 2ª Turma, Data de Julgamento: 14/09/2023. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/trt-23/1969279116>.





APELAÇÃO. AÇÃO CIVIL PÚBLICA. PRELIMINAR DE NEGATIVA DE PRESTAÇÃO JURISDICIONAL. REJEITADA. COMERCIALIZAÇÃO DE PRODUTOS E FERRAMENTAS DE TRATAMENTO DE DADOS PESSOAIS. PROTEÇÃO DOS DIREITOS DO CONSUMIDOR. INOBSERVÂNCIA DA LEGISLAÇÃO DE REGÊNCIA.

1. Apelação interposta contra sentença que, em sede de ação civil pública, julgou procedente a pretensão formulada pelo Ministério Público para condenar a requerida a se abster de comercializar dados pessoais de consumidores, por meio de duas específicas ferramentas de tratamento de dados, sob pena de imposição das medidas indutivas, coercitivas, mandamentais ou sub-rogatórias necessárias para assegurar o cumprimento de ordem judicial, conforme legislação processual civil.

2. A eventual discrepância entre as teses defendidas pelos litigantes e a interpretação conferida pelo julgador às disposições normativas que disciplinam determinada matéria posta em debate não se confunde com a negativa de prestação jurisdicional.

3. Se o que está em pauta é a comercialização de dados tratados, resta evidente que as condições do tratamento – em todas as dimensões do conceito legal – devem ser examinadas.

4. A Lei nº 13.709/2018 (LGPD) dispõe que eventual dispensa da exigência do consentimento do titular das informações processadas não desobriga os agentes de tratamento das obrigações de garantir transparência acerca de todo o processo (coleta dos metadados, da metodologia utilizada, da duração do tratamento, ou do uso compartilhado, por exemplo). A referida norma determina, ainda, que sejam respeitadas a legítima expectativa do titular das informações tratadas e os direitos e liberdades fundamentais. E somente em uma relação de efetiva transparência é possível conceber a existência de legítima expectativa.

5. Mesmo que o produto final dos serviços impugnados garanta ao contratante um apanhado de informações de natureza meramente cadastral, é inafastável a conclusão de que a segmentação e o direcionamento de mercado – prometidos pela requerida – depende de tratamento de informações outras, de natureza socioeconômica e comportamental, elementos intrinsecamente vinculados à esfera da privacidade. Assim, não havendo transparência sobre os trâmites de coleta e tratamento, é impositivo o acolhimento da pretensão autoral.

6. Recurso conhecido e desprovido.



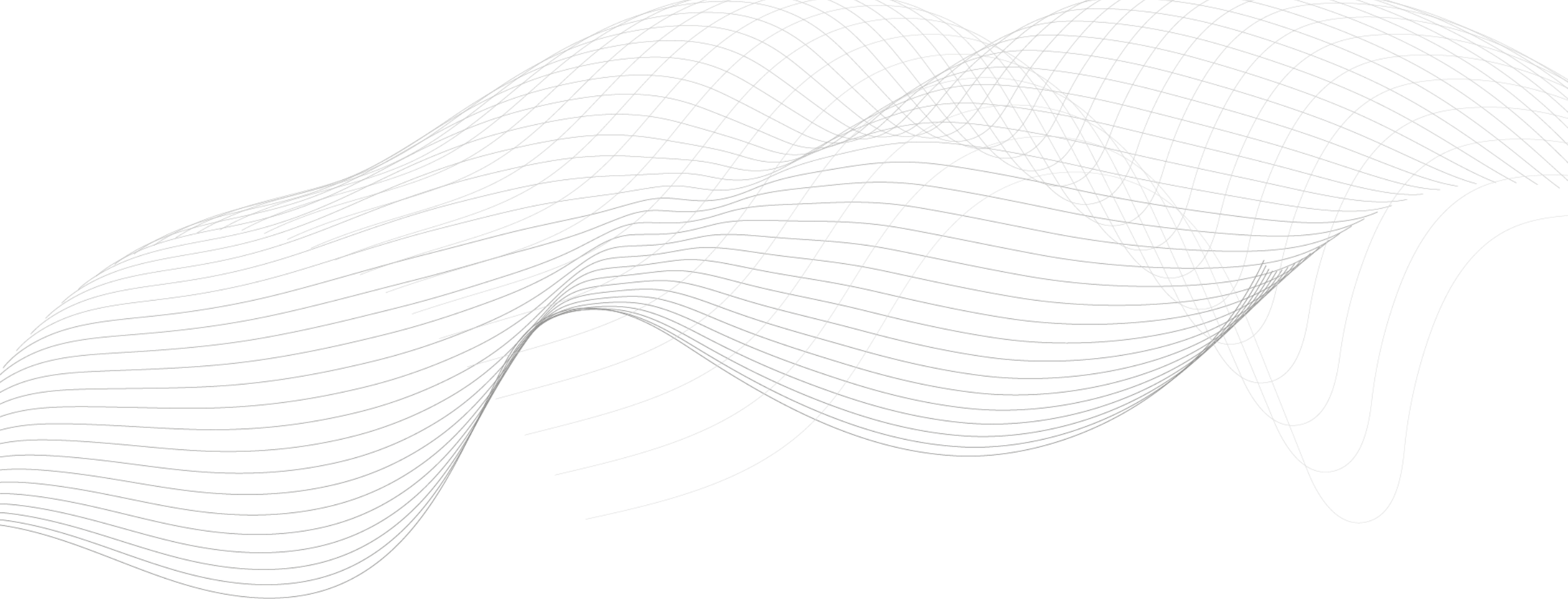
Por conseguinte, mesmo que o tratamento de dados seja necessário à consecução dos objetivos da requerida – e ainda que estes se apresentem em consonância com os fundamentos da livre iniciativa, da concorrência, da inovação e do desenvolvimento econômico e tecnológico – o art. 7º, inciso IX, da LGPD expressamente ressalva os casos em que os dados pessoais tratados reclamem proteção em razão dos direitos e liberdades fundamentais do titular.

Nesse mesmo sentido é o §6º do artigo 7º: “eventual dispensa da exigência do consentimento **não desobriga os agentes de tratamento das demais obrigações previstas nesta Lei, especialmente da observância dos princípios gerais e da garantia dos direitos do titular**”.

O tratamento realizado pela requerida para alcançar listas de potenciais consumidores, além de utilizar informações concernentes a poder aquisitivo, classe social, modelos de afinidade e padrões de consumo – ultrapassando a baliza dos dados de natureza puramente cadastral – não evidencia a necessária transparência aos titulares das informações coletadas.

A requerida, seja nestes autos ou em seu site<sup>[2]</sup>, dirige-se quase que exclusivamente às empresas-clientes; não apresenta aos titulares dos dados tratados todas as informações exigidas no artigo 9º da LGPD. Não há transparência acerca da forma de coleta dos metadados, da metodologia utilizada, da duração do tratamento, ou do uso compartilhado, por exemplo.

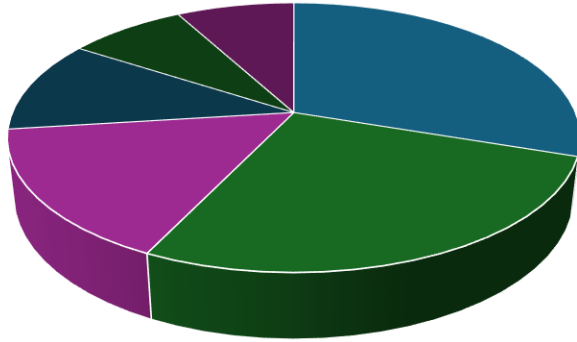
O consumidor precisa ter a exata noção acerca de quais dados pessoais foram utilizados no tratamento, como foram coletados, a forma de processamento e qual a política de compartilhamento, especialmente porque elementos socioeconômicos e comportamentais estão intrinsecamente vinculados à esfera da privacidade e, como tal, reclamam proteção (art. 2º, inciso I, Lei nº 13.709/2018). Não são elementos ou comportamentos plenamente acessíveis ao público ou suscetíveis de serem conhecidos por todos, em absoluto.



# Artigos Mencionados

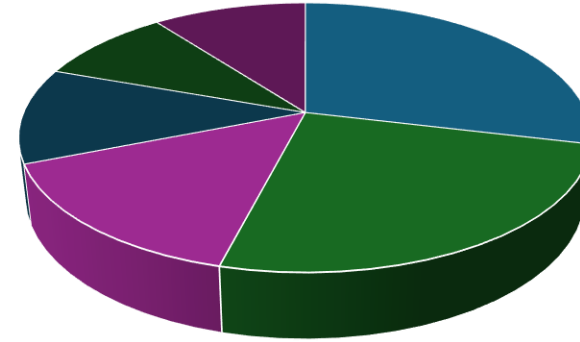
# Artigos Mencionados

1ª Instância



- Definição de Dados Sensíveis (19%)
- Base Legal Proteção ao Crédito (17%)
- Base Legal Exercício Regular de Direitos (10%)
- Bases Legais (7%)
- Objetivos da LGPD (5%)
- Responsab. Reparação Dados (5%)

2ª Instância



- Definição de Dados Sensíveis (25%)
- Base Legal Proteção ao Crédito (22%)
- Base Legal Exercício Regular de Direitos (13%)
- Bases Legais (10%)
- Objetivos da LGPD (8%)
- Responsab. Reparação Dados (9%)

### Dispositivos da LGPD citados: Art. 5º, II.

Trata-se de ação de indenização ajuizada em face de seguradora de seguro de vida, em que o autor alega que foi informado de que seus dados teriam sido acessados por terceiros pela empresa. O autor teve ciência que estelionatários estavam usando seus dados para compras. A sentença foi julgada procedente, mas a empresa apelou alegando a necessidade de comprovação de sua culpa. O TJSP acolheu as razões recursais, concluindo pela **necessidade de avaliar se os dados vazados podem ou não ser considerados como dados sensíveis. Caso não sejam, como era o caso analisado, não se deve condenar a empresa, tendo em vista que não há dado sensível a ser protegido.**

TJSP – Ap. Cív. nº 1008710-70.2021.8.26.0320, Des. Rel. Antonio de Almeida Sampaio, Data de Julgamento: 10/08/2023. Disponível em: <http://www.jusbrasil.com.br/jurisprudencia/1932107452>.

**Dispositivos da LGPD citados: Art. 5º, II; Art. 17; Art. 43; Art. 44; e Art. 45.**

O STJ analisou, em recurso especial, caso semelhante de responsabilização civil de instituição financeira por força de fraude praticada por terceiro contra consumidor. A recorrente **contraiu financiamento de veículo junto a instituição financeira** (recorrida). No intuito de pagar a dívida, foi feito contato via e-mail com esta. Porém, dias depois, a **recorrente foi contatada via aplicativo de mensageria por pessoa que se apresentou como funcionária da recorrente, e, além de comunicar que havia 32 parcelas em aberto, enviou boleto para quitação do empréstimo**. Ao efetuar o pagamento da quantia, a recorrente foi vítima do **“golpe do boleto”**. Em razão da fraude, a instituição financeira não deu quitação da dívida. Por isso, pretendeu a recorrente a declaração da inexigibilidade do débito e da validade do pagamento realizado, bem como a condenação da recorrida a restituir os valores excedentes, com fundamento na responsabilidade pelo fato do serviço. No mérito, **o STJ entendeu que houve vazamento de dados pessoais da recorrente, visto que dados vinculados a operações e serviços bancários são sigilosos** (Art. 1º, Lei Complementar nº 105/2001). Concluiu-se que **“o tratamento indevido de dados pessoais bancários configura defeito na prestação de serviço, notadamente quando tais informações são utilizadas por estelionatário para facilitar a aplicação de golpe em desfavor do consumidor”**. O Tribunal, por fim, aplicou o regime de responsabilidade objetiva por fato do serviço (Art. 14, CDC), fazendo remissão, inclusive, ao Art. 45 da LGPD.

STJ – REsp nº 2.077.278/SP, Rel. Min.<sup>a</sup> Nancy Andrighi, Data de Julgamento: 03/10/2023<sup>68</sup>. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/stj/2108107287>.

# Artigos Mencionados

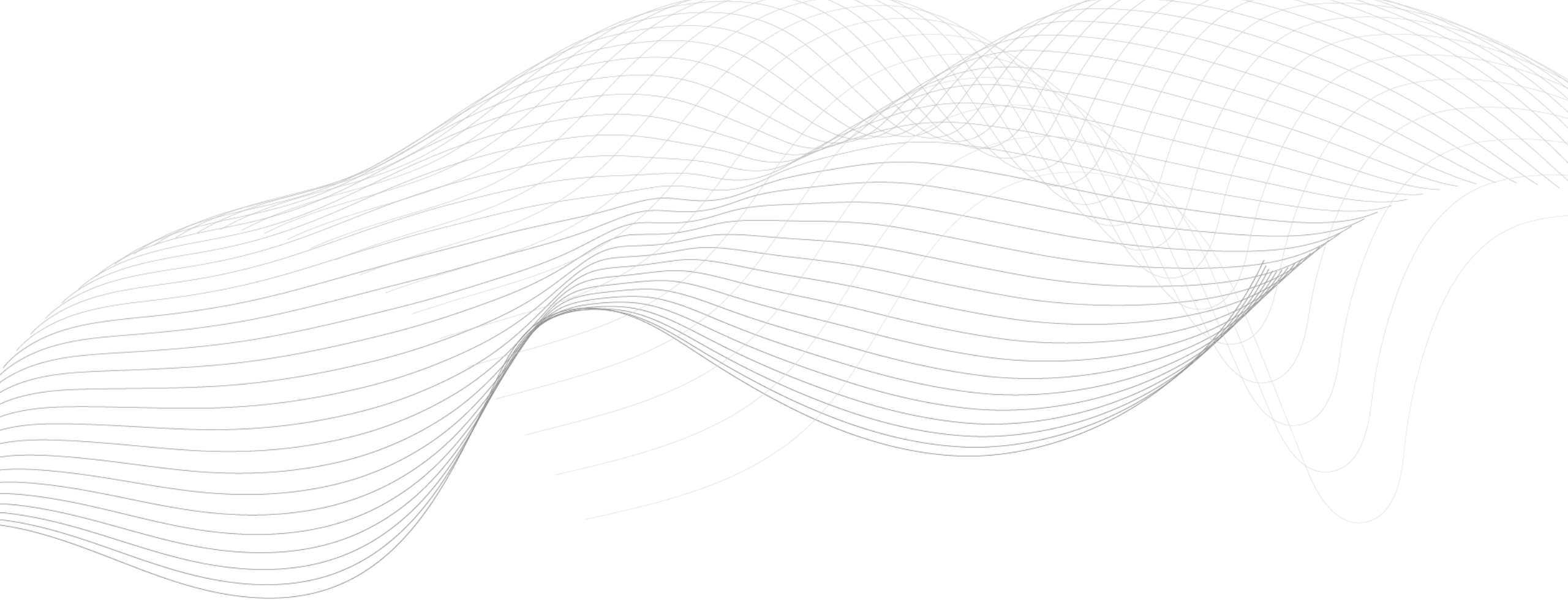
Proteção ao Crédito e  
Prevenção à Fraude

**Dispositivos da LGPD citados: Art. 7º, X, §3º e §4º; Art. 11, II, g.**

Trata-se de ação de obrigação de fazer, cumulada com pedido de indenização por danos morais e pedido de tutela de urgência, ajuizada por titular contra uma empresa, alegando o **uso e comercialização de dados pessoais sem a sua autorização e/ou consentimento**. Como fundamento, entendeu-se que a discussão não envolvia a aplicação da Lei nº 12.414/11 e que os dados pessoais envolvidos seriam cadastrais e, portanto, não são dados pessoais sensíveis. Indicando o Art. 7º, §§ 3º e 4º, o TJSP entendeu pela legalidade da atividade de tratamento da empresa, afirmando que a atividade se refere a elaboração de **“relatório de acesso restrito a pessoas jurídicas, clientes da requerida, com a finalidade exclusiva de proteção ao crédito”**, de acordo com o Art. 7º, X, da LGPD. Ressaltou que os dados envolvidos são necessários para “verificação e confirmação de dados cadastrais” e ainda “maior segurança nas negociações”. Por fim, citou a Súmula 550 do STJ e negou o pedido de indenização formulado pelo titular.

TJSP, Procedimento Comum Cível nº 1021791-76.2022.8.26.0506, Des. Rel. Loredana de Carvalho, 6ª Vara Cível, Data de Julgamento: 02/11/2022. Disponível em: <http://www.jusbrasil.com.br/jurisprudencia/1779706142>.



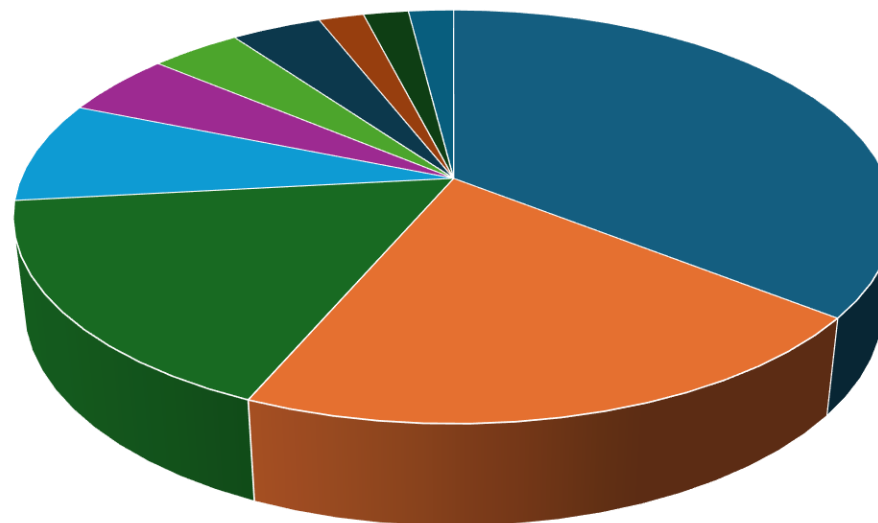


# Bases Legais



# Bases Legais

Base Legal



- Proteção ao Crédito (36%)
- Exercício regular de direito (21%)
- Consentimento (17%)
- Obrigação Legal (8%)
- Legítimo Interesse (5%)
- Execução de Contrato (4%)
- Realização de Estudos (4%)
- Tutela da Saúde (2%)
- Políticas Públicas (2%)
- Proteção da Vida (2%)

### Dispositivos da LGPD citados: Art. 2º, I a VII; Art. 7º, I, V, IX, §4º.

Trata-se de caso em que um sindicato ajuizou ação de cumprimento contra a empresa buscando o cumprimento de cláusula normativa. Defendeu que a empresa se recusou a “fornecer a relação de funcionários atualizada, com a indicação de data de admissão, CPF e salário, com o fim de aferir se os benefícios sociais advindos da norma coletiva estão sendo cumpridos”. O Tribunal acatou a defesa da empresa em justificar o não compartilhamento dos dados por ausência de consentimento específico dos empregados, citando os fundamentos da LGPD previstos no Art. 2º e os dispositivos referentes ao consentimento do Art. 7º. Com base no Art. 611-A da CLT, considerou-se que “a norma coletiva tem prevalência sobre a legislação trabalhista, mas não sobre os direitos individuais do trabalhador” e, diante do requisito da norma coletiva sobre a exigência do consentimento dos empregados para compartilhamento de seus dados sensíveis ao sindicato, “se faz necessário que o Sindicato obtenha autorização expressa e específica do trabalhador”. Assim, a conduta da empresa foi considerada apropriada, indicando-se também como fundamento o Art. 5º, II, da Constituição.

TRT2 – ATSum nº 1000315-38.2023.5.02.0482, Rel. Des. Adriana Pita Colella, 2ª Vara do Trabalho de São Vicente, Data de Julgamento 25/08/2023. Disponível em: <http://www.jusbrasil.com.br/jurisprudencia/1943328997>.



# Bases Legais

Execução de Contrato -  
Legítimo Interesse

encontra 100% em português, como se verifica às fls. 1620. Os autores insistem na suposta ausência de base legal para o tratamento de dados pelo Telegram com base na LGPD, argumentando que o consentimento seria a única base legal para o tratamento de dados pela 1ª ré, de acordo com o arts. 7º, I, e 11, I, da LGPD. Entretanto, o consentimento não é a única ou a principal base legal para permitir o tratamento de dados pessoais nos termos da LGPD, pois nesta são elencadas 10 (dez) bases legais possíveis para fundamentar o tratamento de dados pessoais, 9 (nove) das quais não envolvem ou exigem o consentimento do usuário. Ressalte-se que dentre essas 10 (dez) bases legais, não há hierarquia, e o consentimento não é a principal base legal para o tratamento de dados nos termos da LGPD e/ou de outra lei aplicável no Brasil. Dessa forma, o tratamento de dados é legítimo quando justificado ou enquadrado em qualquer uma das bases legais definidas na LGPD, ainda que o controlador dos dados opte por não basear o tratamento do dado no consentimento do usuário. Além disso, a prestação dos serviços de mensageria é de interesse dos consumidores, pois estes



### Dispositivos da LGPD citados: Art. 5º, II; Art. 7º, VI; Art. 11, II, d.

Ação de produção antecipada de prova com pedido de exibição de documentos de registro de “todos os empregados e atividade e os já dispensados” formulada por sindicato. O pedido foi recusado pela empresa alegando que as informações seriam dados pessoais sensíveis, nos termos do Art. 5º, II, da LGPD; há vedação pelo Art. 16 do Decreto 10.854/2021, com exclusividade de requerimento das informações aos Auditores-Fiscais do Trabalho; há vedação pela Convenção Coletiva da Categoria; e juntou termo de recuso de fornecimento dos documentos de 75 funcionários. A decisão reconhece a legitimidade e interesse de agir do sindicato “ao pleitear a apresentação de documentos relativos aos integrantes da categoria”, entendendo ser permitida a apresentação dos documentos solicitados a partir da hipótese legal para exercício regular de direitos (Art. 7º, VI e Art. 11, II, d, da LGPD). Considera-se ainda que a responsabilidade pelo “tratamento, guarda e disponibilidade dessas informações” são do sindicato, por requerem acesso para disponibilização dos documentos em processo judicial. Por fim, determina que “a empresa requerida deverá juntar os documentos de forma sigilosa, com restrição de visibilidade e acesso somente às partes e seus advogados”, diante da existência “de dados potencialmente sensíveis” e como meio de proteger os dados pessoais de terceiros.

TRT24 – PAP nº 0025007-25.2022.5.24.0003, Rel. Des. Leonardo Ely, Vara do Trabalho de Fátima do Sul, Data de Julgamento: 13/06/2023. Disponível em: <http://www.jusbrasil.com.br/jurisprudencia/1865064023>.



### Dispositivos da LGPD citados: Art. 7º, VI; Art. 11, II, d; Art. 50, X.

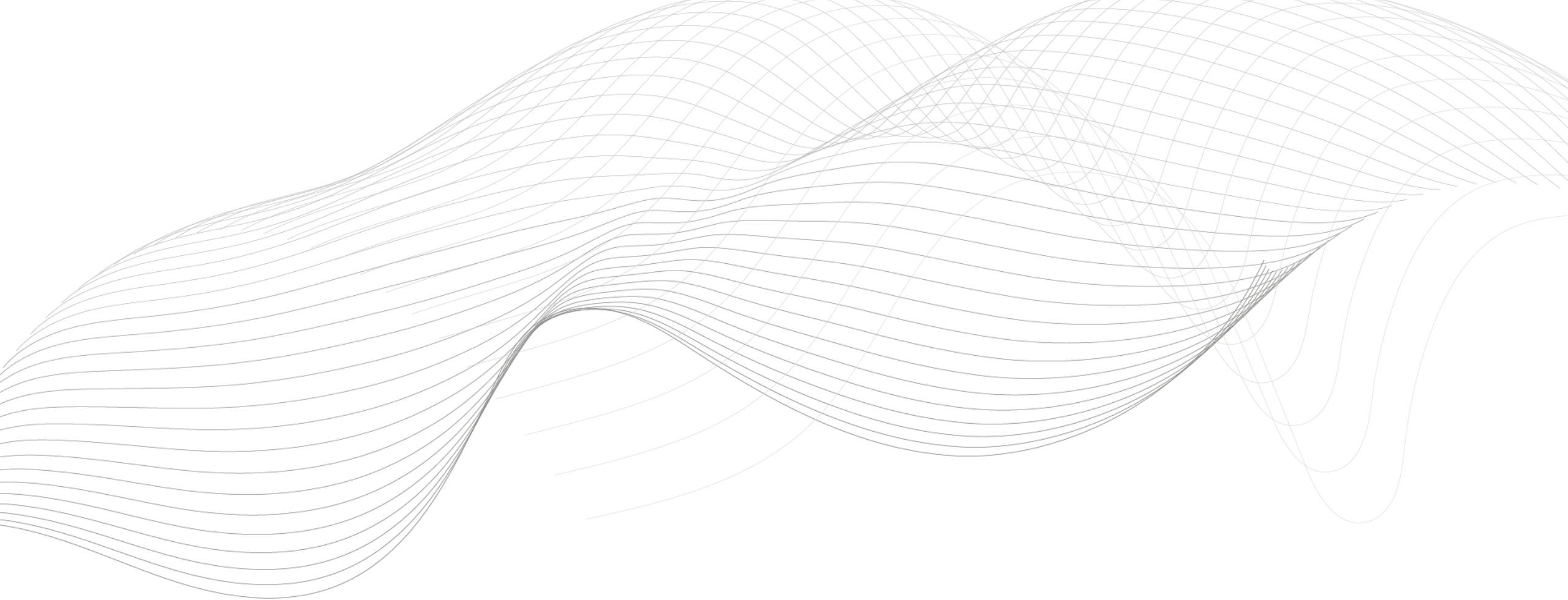
No caso, uma das partes se manifestou contra a juntada de documentos que comprovem o preenchimento dos pressupostos legais para a **concessão de gratuidade**, defendendo a suficiência da declaração de hipossuficiência e a inviolabilidade do sigilo bancário e fiscal. O TJMS concluiu que a presunção de insuficiência não é absoluta, cabendo ao juiz oportunizar a comprovação do preenchimento dos requisitos, com a possibilidade de ele ser negado. Em complemento, considerou-se que **o sigilo dos dados pessoais, indicado enquanto justificativa para negar a apresentação dos documentos, é "inoponível ao Poder Judiciário no exercício de sua função jurisdicional, sobretudo quando os dados são necessários para consecução de direito previsto em lei"** (no caso, o direito ao benefício da justiça gratuita)". Assim, indicam-se os Arts. 7º, X e 11, II, g, da LGPD, que permitem o tratamento de dados pessoais, "inclusive sem fornecimento de consentimento do titular", no âmbito processual. Considerando que nos autos "existem evidências da suficiência de recursos do apelante", o pedido de gratuidade da justiça foi indeferido.

TJMS, Apelação nº 081449-58.12.015.8.12.0001, Rel. Des. Paulo de Oliveira, 3ª Câmara Cível, Data de Julgamento: 07/06/2023. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/tj-ms/1866005957/inteiro-teor-1866005962>.

**Dispositivos da LGPD citados: Art. 5º, incisos I e II; Art. 7º, incisos II a X, §3º, §4º.**

Trata-se de apelação cível contra sentença que julgou improcedente a ação de obrigação de fazer, cumulada com pedido de indenização por danos morais, ajuizada por titular de dados. No caso, a divulgação dos dados pessoais do titular (nome completo, número de CPF, data de nascimento, nome da mãe, sexo, endereço e telefone) ocorreu sem sua autorização e/ou notificação prévia. Em sede de apelação, o TJSP considerou que, no caso, incide a base legal do Art. 7º, X, da LGPD e, por isso, o consentimento não é necessário. Além disso, **pondera-se que as informações coletadas são públicas e não são excessivas ou dados sensíveis, "obtidas por meios lícitos, dentro de sua autorizada atuação na área de proteção ao crédito, ausente prova em sentido contrário ou demonstração de comercialização ou divulgação indevida"**. Com relação à jurisprudência prévia indicada, há destaque para o **Tema 710 e Súmula 550 do Superior Tribunal de Justiça** sobre o sistema **"credit scoring"** e a dispensa do consentimento do titular. Portanto, o recurso da titular não foi provido.

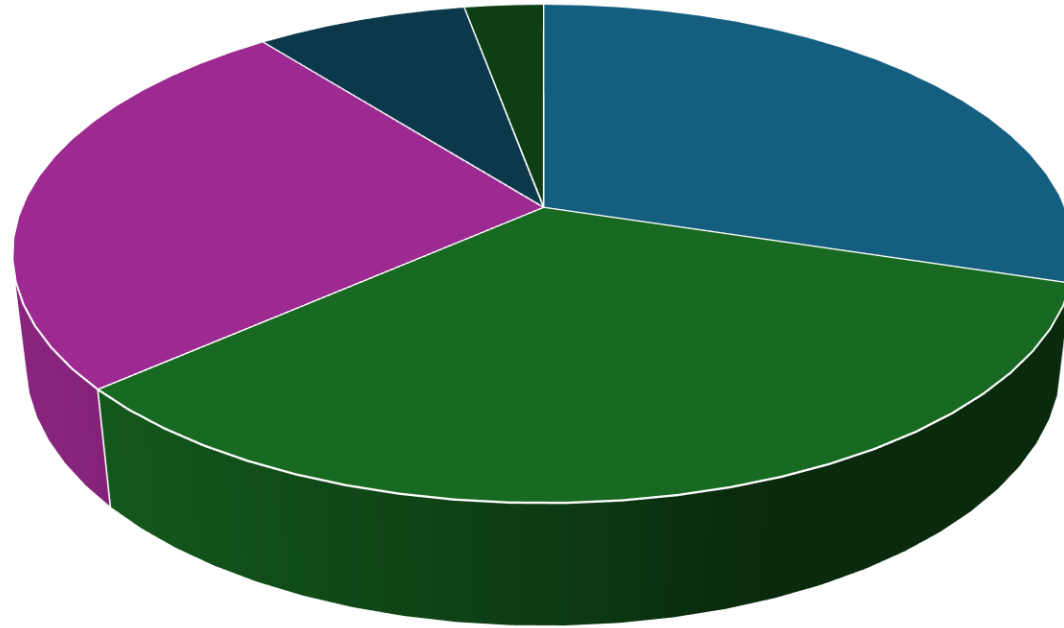
TJSP – Apelação Cível nº 1000460-97.2022.8.26.0648, Des. Rel. Cauduro Padin, 13ª Câmara de Direito Privado, Data de Julgamento: 13/04/2023. Disponível em: <https://www.iusbrasil.com.br/jurisprudencia/tj-sp/1811528175>.



# Direitos dos Titulares

# Direitos dos Titulares

Direitos



- Decisões Automatizadas - Art. 20 (31%)
- Acesso a Informações - Art. 9º (27%)
- Conceito Anonimização - Art. 5º, IX (3%)
- Direito dos Titulares - Art. 18 (35%)
- Revogação do Consentimento - Art. 8º (4%)



### Dispositivos da LGPD citados: Art. 18, II.

O acórdão julgou recurso nominado interposto pelo autor, pessoa física, em face da sentença que julgou improcedente seu pedido de condenação da ré, **construtora** imobiliária, para **informar quais foram os dados e os bancos de dados utilizados na avaliação da formação do contrato de aquisição de unidade imobiliária de empreendimento**. O voto descreve que a ré **não possui obrigação legal** de fornecer as informações solicitadas, **tendo em vista que a venda a crédito está sim na esfera de discricionariedade da atividade da fornecedora, desde que não haja tratamento discriminatório ou preterição de qualquer ordem**". Ainda, o voto afirma que **"ré não se enquadra nos conceitos de controladora ou operadora das quais poderia se exigir informações dos dados constantes de seu cadastro interno. A ré é simplesmente uma empresa privada que oferece no mercado de consumo a venda de unidades imobiliárias, não sendo titular nem administradora de qualquer órgão ou cadastro público ou privado de dados, nos termos da Lei nº 13.709/18"**. Nota-se que o voto proferiu interpretação restritiva de quem poderia exercer função de controlador de dados e da concretização de direito de acesso.

TJPR – Processo nº 0044368-02.2021.8.16.0014, Rel. Vanessa Bassani, 1ª Turma Recursal, Data de Julgamento: 30/09/2022. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/tj-pr/1726923350>.



### Dispositivos da LGPD citados: Art. 18, IV.

O acórdão julgou recurso inominado interposto contra sentença que determinou a exclusão de forma definitiva os dados do autor dos seus sistemas internos. Um dos recorrentes afirma que as informações constantes no cadastro interno possuem somente o objetivo de nortear o perfil do cliente, não tendo caráter público, de forma que não deveriam ser excluídas. No entanto, o relator destaca que “quanto à exclusão dos dados do recorrido do sistema interno do recorrente [...], trata-se de direito do titular dos dados. **A contratação se deu mediante fraude, de modo que não foi obtido por meio de seu titular e com o seu consentimento. Dessa forma, é direito assegurado no Art. 18, IV da Lei 13.709/2018 a eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei, desde que mediante solicitação**”. Com isso, o acórdão entende que dados obtidos por fraude estão em desconformidade com a LGPD e podem ser excluídos por requisição do titular.

TJSP – Processo nº 1010111-56.2022.8.26.0066, Rel. Ayman Ramadan, Segunda Turma Cível, Data de Julgamento: 13/09/2023. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/tj-sp/1971244153>.

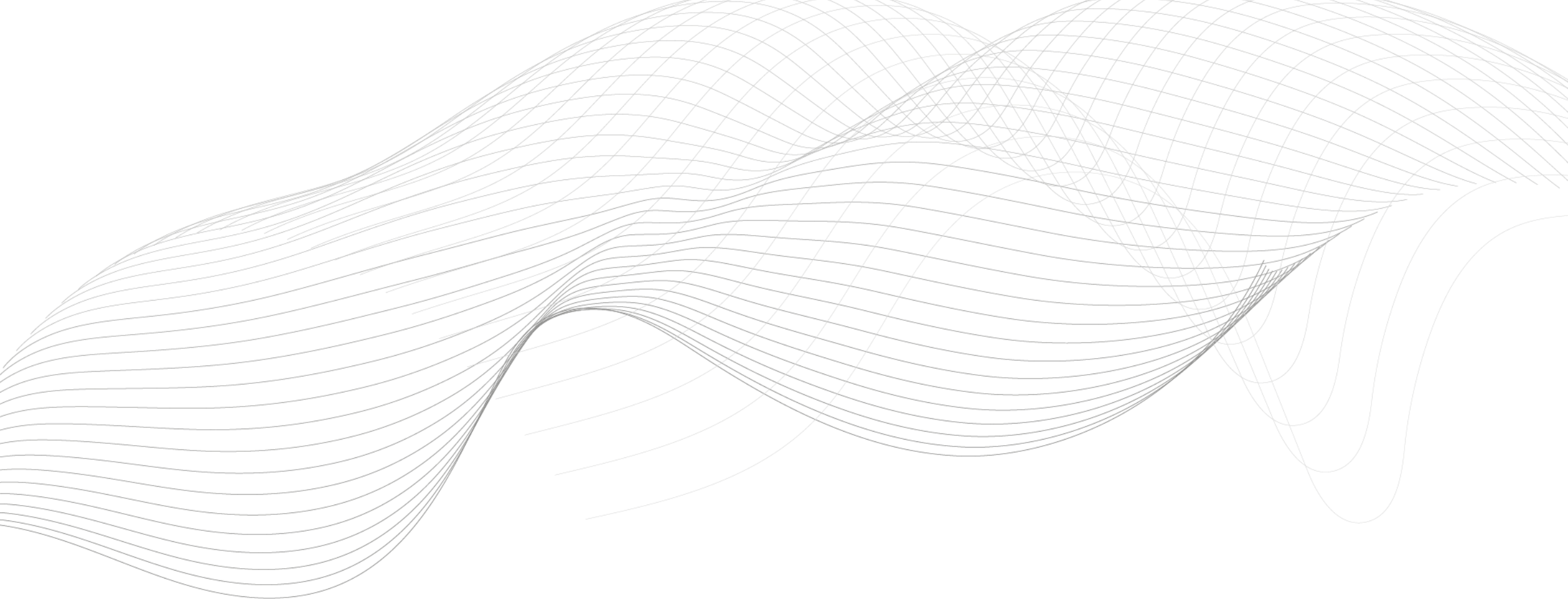


### Dispositivos da LGPD citados: Art. 20, caput.

O acórdão julgou uma apelação contra a sentença de improcedência de dano moral e material derivado do cancelamento do contrato de prestação de serviço de transporte por aplicativo. A autora, apelante, argumentou que a ré, empresa de transporte por aplicativo, não lhe oportunizou a revisão da decisão, que foi baseada, exclusivamente, em seu sistema automatizado, olvidando o disposto no artigo 20, da Lei Geral de Proteção de Dados. O relator cita que “o descredenciamento da apelante da plataforma gerida pela apelada se deu, segundo alegado na contestação, pelo fato de a apelante ter compartilhado sua conta com terceiros, fato que teria sido verificado por meio do sistema de identificação facial. Além disso, a apelada asseverou que, nos termos contratados, é lícita a rescisão do contrato, independentemente de aviso prévio. A apelante afirmou em réplica que a mudança de sua aparência, conforme se verifica da comparação entre as fotografias copiadas, se deu em razão da realização de cirurgia bariátrica.” O relator, no entanto, entendeu que “não há notícia de que requereu alguma providência destinada a reverter a suspensão que lhe foi imposta, em que pesa sustentar em Juízo que tinha direito de postular a revisão da suspensão com base no artigo 20, da Lei n.º 13.709/2018”. Dessa forma, para o magistrado, seria necessário que a autora, primeiro, solicitasse direito de revisão em face da empresa ré. Apenas após a negativa da empresa, a autora poderia alegar o direito em juízo.

TJSP, Processo nº 1064766-70.2022.8.26.0100, Rel. Sá Duarte, 33ª Câmara de Direito Privado, Data de Julgamento: 18/04/2023. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/tj-sp/1815906688>.





# Responsabilidade Civil

# Responsabilidade Civil

Um dos assuntos mais recorrentes nas decisões analisadas foi a responsabilidade civil, especialmente quanto à reparação de danos pelos agentes de tratamento (14%).

O dano moral foi mais mencionado que o dano patrimonial, como demonstrado abaixo:

	DANO MORAL	DANO PATRIMONIAL
1º GRAU	20%	8%
2º GRAU	33%	14%

# Dano Moral em Incidentes de Segurança

## CORRENTE 1

**Danos Morais ocasionados por incidentes de segurança possuem natureza in re ipsa:**

De acordo com essa corrente, o mero incidente com dados pessoais (incluem-se aqui, em sua maioria, incidentes de vazamento) é capaz, por si só, de ocasionar dano moral. Logo, não seria necessário comprovar ocorrência e extensão do dano para ensejar condenação à reparação.

## CORRENTE 2

**Danos Morais ocasionados por incidentes de segurança não possuem natureza in re ipsa:**

Segundo essa corrente, o mero incidente com dados pessoais (incluindo, em sua maioria, incidentes de vazamento) não é capaz de ocasionar dano moral. Portanto, seria necessário comprovar a ocorrência e extensão do dano moral para ensejar a obrigação de sua reparação.

Essa corrente é a mais aceita: corroborando esse entendimento, uma decisão do Superior Tribunal de Justiça (STJ) proferida em 7 de março de 2023 pelo Min. Francisco Falcão nos autos do AREsp 2130619/SP estabeleceu que não se presume dano moral decorrente de vazamento de dados pessoais comuns (i.e. nome, sobrenome e informações básicas de registro), sendo necessário que o titular dos dados comprove o efetivo prejuízo gerado pela exposição dessas informações.



**Dispositivos da LGPD citados: Art. 5º, II; Art. 42; Art. 43, I e III; Art. 46; Art. 48.**

O caso discute a existência da obrigação de indenização por dano moral presumido à pessoa que foi vítima de um incidente de segurança, mais especificamente de um vazamento de dados. No caso, a pessoa que teve seus dados pessoais vazados requereu indenização a título de danos morais à empresa responsável pelo incidente. No entanto, a Segunda Turma do STJ firmou entendimento no sentido de que, apesar de ser uma falha no tratamento de dados, o fato de os dados da autora terem sido expostos não seria suficiente para gerar dano moral indenizável. Essa obrigação surgiria apenas nos casos em que o titular dos dados comprovasse eventual dano decorrente da exposição dessas informações. Além disso, a Turma entendeu que os dados objeto do vazamento são dados não sensíveis, de forma que o direito de personalidade da autora não seria afetado se terceiros acessassem esses dados. Como eles são informados corriqueiramente, o seu vazamento não é suficiente para gerar dano moral indenizável. Logo, neste julgamento, o STJ entendeu que o vazamento de dados não sensíveis não gera dano moral indenizável presumido, ou seja, se não houver comprovação do dano.

STJ – AREsp nº 2.130.619/SP, Ministro relator: Francisco Falcão, 2ª Turma, Data de Julgamento: 07/03/2023. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/stj/1780119718>.



### Dispositivos da LGPD citados: Art. 1º.

O caso versa sobre existência de **dano moral indenizável diante de vazamento de dados** pessoais por instituição bancária. O autor da ação, sujeito que teve seus dados vazados, alegou que a empresa ré deveria ser condenada a pagar indenização por não ter mantido seus dados pessoais em local seguro e fora do alcance de terceiros. A partir do vazamento, o autor alega que “passou a ser assediado por empresa especializada na negociação de consórcio, a qual se utilizou das suas informações pessoais e ofereceu determinada quantia pela compra de crédito”. No entanto, a 5ª Câmara Cível do TJMS concluiu que **a obrigação de indenizar apenas surge com a comprovação de que ocorreu algum dano concreto, não potencial**. Assim, apesar do autor ter comprovado o vazamento de dados, o Tribunal entendeu que não houve demonstração de alguma situação fática vexatória causada pela utilização de seus dados para oferta de serviços de terceiros, de forma a não ser possível configurar danos morais. Para o tribunal, seria **configurado dano se os dados pessoais fossem utilizados para prática de fraude**. Dessa forma, o tribunal determina que “a mera constatação de que dados pessoais básicos tenham sido objeto de ilegal vazamento não configura, automaticamente, dano moral; sendo certo que não há nos autos prova de outras reverberações do referido compartilhamento irregular”.

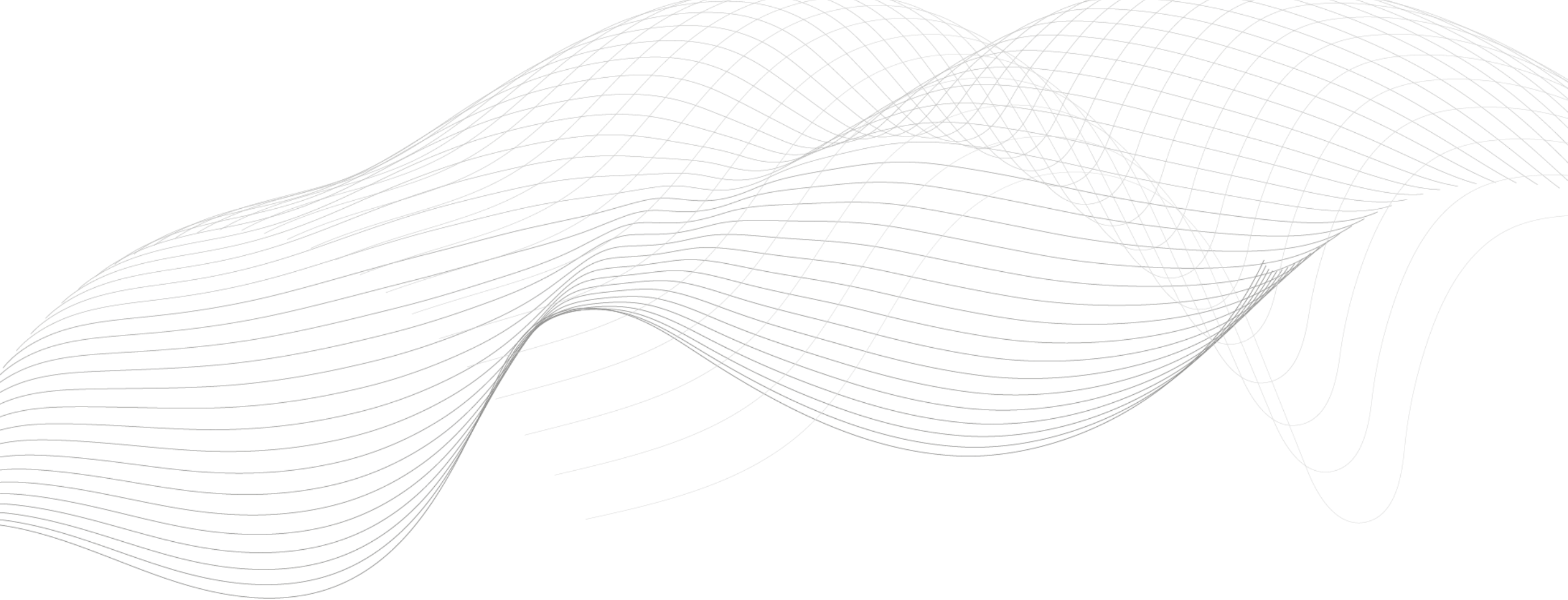
TJMS, Apelação Cível nº 0803059-55.2021.8.12.0021, Des. Rel. Geraldo de Almeida Santiago, Data de Julgamento: 16/12/2022. Disponível em: <http://www.jusbrasil.com.br/jurisprudencia/1743948775>.



**Dispositivos da LGPD citados: Art. 2º, I a VII; Art. 17; Art. 42; Art. 44; Art. 46.**

No caso, o titular ajuizou ação para reparação por danos morais e recuperação de conta na rede social (Instagram) “que foi hackeada e utilizada por terceiros para vendas fraudulentas”. Para o TJPR, restou configurada a relação de consumo e concluiu-se pela falha na prestação de serviços da empresa, em virtude da exposição da intimidade e dados pessoais sensíveis do titular aos golpistas, “tais como fotografias, conversas particulares e outros que ela tenha optado por manter em sigilo”. Assim, houve ofensa ao direito à proteção de dados pessoais e à autodeterminação informativa, já que o titular ficou prejudicado em exercer “controle sobre suas próprias informações”.

TJPR - Recurso Inominado Cível nº 0034984-93.2021.8.16.0182, Relator (Desembargador): Marcel Luis Hoffmann, 11º Juizado Especial Cível de Curitiba/PR, Data de Julgamento: 10/02/2023. Disponível em: <http://www.iusbrasil.com.br/iurisorudencia/1761047817>.



# Conclusões

# Conclusões

1

## **Há uma tendência à discussão judicial da aplicação das bases legais da LGPD:**

Dentre as decisões analisadas, predominaram as menções às seguintes bases legais: proteção ao crédito (36%), exercício regular de direitos (21%), consentimento (17%), cumprimento de obrigação legal (8%) e legítimo interesse (5%).

2

## **As áreas que mais fizeram intersecção com a proteção de dados foram Direito do Consumidor e Direito Trabalhista:**

Os casos envolvendo direito do consumidor totalizaram 43% das decisões, sendo a maioria voltada para a reparação de danos. Os casos envolvendo direito trabalhista totalizaram 34% das decisões, sendo o assunto principal a produção de provas digitais, dentre os quais, 87% tratam da utilização de dados de geolocalização para comprovação da jornada de trabalho.

3

## **O dano moral por vazamentos de dados não é presumido:**

O STJ tem firmado o entendimento de que o dano moral por vazamento de dados deve ser comprovado, ou seja, não possui natureza in re ipsa (presumido). No entanto, caso o incidente de segurança envolva dados pessoais sensíveis, o entendimento é de que a comprovação não é necessária.

# Conclusões

4

**O direito à revisão de decisões automatizadas é o mais demandado:**

No que se refere aos direitos dos titulares, verificou-se que o direito à revisão de decisões automatizadas (art. 20 da LGPD) foi o mais pleiteado, com citação em 15% das decisões.

5

**A responsabilidade dos agentes de tratamento é um dos principais assuntos:**

Dentre as decisões analisadas, 14% trata da responsabilidade dos agentes de tratamento, sendo a principal discussão a responsabilidade dos agentes em casos de aplicação de fraudes e golpes.

6

**O principal setor envolvido nas demandas são empresas do setor financeiro:**

Os principais setores mencionados nas decisões são: bancos, financeiras e administradoras de cartão (26%); bancos de dados e cadastros de consumidores (18%); e operadoras de telecomunicações (7%).

