# Acesso à informação proteção de dados e privacidade nas Cortes Constitucionais

## pontos de convergência e divergência nos Tribunais Constitucionais brasileiro e alemão

Carlo José Napolitano
Enrico Lentini Gibotti
Lucas Catib de Laurentiis
Sarah Thiemy Kawato dos Santos
Tatiana Stroppa
(Orgs.)

Pedro & João editores

# Acesso à informação proteção de dados e privacidade nas Cortes Constitucionais:

## pontos de convergência e divergência nos Tribunais Constitucionais brasileiro e alemão

Pedro & João
editores

**Equipe do projeto**

O projeto de pesquisa está sendo desenvolvido no Grupo de Pesquisa Mídia e Sociedade/CNPq, na linha de pesquisa Direito à Comunicação: http://dgp.cnpq.br/dgp/espelhogrupo/4162952981530090 e conta com a equipe que segue:

**Coordenador**

Prof. Ass. Carlo José Napolitano
Departamento de Ciências Humanas, da Faculdade de Arquitetura, Artes, Comunicação e Design, Unesp/Bauru e Programa de Pós-graduação em Comunicação, UNESP/Bauru.

**Pesquisadores Associados**

Prof. Dr. Lucas Catib de Laurentiis
Faculdade de Direito da Pontifícia Universidade Católica de Campinas e Programa de Pós-Graduação Direito/PucCamp

Prof. Dra. Tatiana Stroppa
Centro Universitário de Bauru (ITE-SP), Faculdade Iteana de Botucatu
Pós-Graduação Direito/ITE

**Participantes do Projeto**

Ana Carolina Brandão da Silva
Arthur Almeida de Oliveira
Audrey Sabbatini
Deborah Cunha Teodoro
Enrico Lentini Gibotti
Felipe de Oliveira Mateus
Greici Maria Zimmer
Guilherme Lima Zanin
Isadora Pinto de Sousa
Laura Santos Lopes
Luiz Henrique Ranzani
Luize D'Alessandro De Paula
Matheus Ramalho Orlando
Milena Fernanda De Brito
Natanaelle Gomes
Pedro Martins
Régis Martins
Renato Sobhie Zambonatto
Rodrigo Nery de Né
Samara Meneses Brito
Sarah Thiemy Kawato dos Santos

**Carlo José Napolitano**
**Enrico Lentini Gibotti**
**Lucas Catib de Laurentiis**
**Sarah Thiemy Kawato dos Santos**
**Tatiana Stroppa**
**(Organizadores)**

# Acesso à informação proteção de dados e privacidade nas Cortes Constitucionais:

## pontos de convergência e divergência nos Tribunais Constitucionais brasileiro e alemão

**Apoio:**

CNPq
Conselho Nacional de Desenvolvimento Científico e Tecnológico

Pedro & João editores

**Carlo José Napolitano; Enrico Lentini Gibotti; Lucas Catib de Laurentiis; Sarah Thiemy Kawato dos Santos; Tatiana Stroppa [Orgs.]**

**Acesso à informação proteção de dados e privacidade nas Cortes Constitucionais: pontos de convergência e divergência nos Tribunais Constitucionais brasileiro e alemão.** São Carlos: Pedro & João Editores, 2024. 128p. 16 x 23 cm.

**ISBN: 978-65-265-1630-0 [Digital]**

**DOI: 10.51795/9786526516300**

1. Direito à informação. 2. Liberdade de expressão. 3. Proteção de dados. 4. Acesso à Internet. I. Título.

CDD – 340/370

**Capa:** Marcos Della Porta
**Ficha Catalográfica:** Hélio Márcio Pajeú – CRB - 8-8828
**Diagramação:** Diany Akiko Lee
**Editores:** Pedro Amaro de Moura Brito & João Rodrigo de Moura Brito



**Pedro & João Editores**
www.pedroejoaoeditores.com.br
13568-878 – São Carlos – SP
2024

# Agradecimentos

Agradeço inicialmente aos parceiros Tatiana Stroppa e Lucas Catib de Laurentiis por terem aceito prontamente participar do projeto de pesquisa. Agradeço também aos alunos, membros da linha de pesquisa Direito à Comunicação, do grupo Mídia e Sociedade, pela colaboração na pesquisa e na elaboração deste material. Agradeço as instituições parceiras, ITE e PucCamp. Agradeço ao CNPq pelo financiamento do projeto de pesquisa, bem como para a edição deste e-book. Meu muito obrigado a todos!

Carlo José Napolitano

# Sumário

Introdução 9
*Carlo José Napolitano*
*Lucas Catib de Laurentiis*
*Tatiana Stroppa*

Apresentação 25
*Enrico Lentini Gibotti*
*Lucas Catib de Laurentiis*
*Sarah Thiemy Kawato dos Santos*

**EIXO COMPARTILHAMENTO DE DADOS**

Protegendo o Estado de movimentos terroristas: qual é o limite? 33
*Enrico Lentini Gibotti*
*Samara Meneses Brito*

Análise do compartilhamento de dados e proteção de privacidade no STF 49
*Régis Martins*
*Samara Meneses Brito*

**EIXO INVESTIGAÇÃO CRIMINAL**

O sigilo de dados e a garantia da privacidade nas investigações criminais 65
*Carlo José Napolitano*
*Deborah Cunha Teodoro*
*Isadora Pinto de Sousa*
*Tatiana Stroppa*
*Lucas Catib Laurentiis*

**EIXO DIVULGAÇÃO DE PROCESSOS**

Limites do Direito à Informação diante das novas tecnologias: reflexões sobre a publicidade processual em ambientes digitais a partir do Tema 1141 do STF 79
*Arthur Almeida de Oliveira*
*Renato Sobhie Zambonatto*

**EIXO BANCO DE DADOS**

Acesso a informações nos bancos de dados da Receita Federal: governança de dados e privacidade 101
*Carlo José Napolitano*
*Deborah Cunha Teodoro*
*Lucas Catib Laurentiis*
*Tatiana Stroppa*

**EIXO PROTEÇÃO DE DADOS**

Proteção de dados e os meios de telecomunicações na realidade alemã: uma análise de caso 113
*Laura Santos Lopes*
*Luiz Henrique Ranzani*
*Sarah Thiemy Kawato dos Santos*

Conclusão 123
*Carlo José Napolitano*
Equipe do projeto

Autores 127

# Introdução

Carlo José Napolitano
Lucas Catib de Laurentiis
Tatiana Stroppa

Este e-book apresenta resultados parciais da pesquisa "A liberdade de expressão na internet e a proteção dos direitos da personalidade no ambiente *online*: análise comparativa de decisões do Supremo Tribunal Federal e do Tribunal Constitucional Federal Alemão"[1], projeto financiado pela Chamada Universal, Edital 18/2021, Faixa A – Grupos Emergentes do Conselho Nacional de Desenvolvimento Científico e Tecnológico – CNPq, processo 403756/2021-9[2].

A proposta submetida à Chamada Universal, Edital 18/2021, propôs investigar a liberdade de expressão na internet e a proteção dos direitos da personalidade *online* no Brasil e na Alemanha, em especial, as orientações e interpretações conferidas pelo Supremo

[1] O projeto que aqui se relata é um desdobramento da participação do coordenador no projeto de cooperação internacional **"Comunicação e democracia: responsabilidade da mídia, mídia de serviço público, acesso à Internet e direito à informação na Alemanha e no Brasil",** financiado pelo Programa CAPES/DAAD – PROBRAL, Processo 88887.371422/2019-00.

[2] A linha de pesquisa Direito à Comunicação, criada em 2015, contou, até a edição deste e-book, com a participação de 37 estudantes de graduação e pós-graduação. Atualmente são 18 alunos e ex-alunos atuantes (doutores, doutorandos, mestres, mestrandos e graduandos), da Unesp, Instituição Toledo de Ensino e PucCampinas. Como resultado de formação de recursos humanos, especificamente em relação ao projeto, já temos 5 iniciações científicas com bolsa concluídas, sendo uma delas no exterior, 1 IC sem bolsa concluída e 3 IC com bolsa em andamento, além de mestrados e doutorados que se relacionam ao projeto. Também em decorrência das parcerias entre PucCampinas, Instituição Toledo de Ensino e Unesp, em 2023, criamos um Núcleo de Pesquisa, denominado Núcleo de Pesquisa de Direito à Comunicação e desenvolvemos um site para divulgação das produções científicas do grupo, que pode ser acessado em: nupedic.com.br

Tribunal Federal (STF) e pelo Tribunal Constitucional Alemão (TCF) sobre essas temáticas.

O objetivo principal e substancial, portanto, era analisar, comparativamente, decisões do STF e do TCF sobre a liberdade de expressão na internet e a proteção dos direitos da personalidade *online*, no intuito de verificar se seria possível identificar uma linha mestra, ou, em outros termos, um *modus operandi* de interpretação do STF/TCF relacionado à temática proposta.

Diante disso, a pesquisa objetivou responder ao seguinte problema de pesquisa: **Como o STF/TCF decide(m) as ações relacionadas à liberdade de expressão na internet e a proteção dos direitos da personalidade no ambiente virtual (*on-line*)?**

Sabe-se que o Direito brasileiro protege a liberdade de expressão na internet, resguardando os direitos da personalidade. O Marco Civil da Internet (2014) e a Lei Geral de Proteção de Dados (2018) são exemplos relevantes. Por sua vez, no Direito Alemão, a Lei Federal de Proteção de Dados (Bundesdatenschutzgesetz-BDSG, 2017) e a Lei de Aplicação da Rede (Netzwerkdurchsetzungsgesetz – NetzDG, 2017) são os principais marcos legais.

Observe-se que a jurisprudência do TCF reconhece, desde a década de 1980, o direito à autodeterminação informativa, ou dito de outro modo, o direito fundamental à proteção de dados, que consiste no "poder do indivíduo em determinar fundamentalmente por si mesmo sobre a coleta e utilização de seus dados pessoais" (Mendes, 2018, p. 188). Direito esse intimamente conectado aos direitos de personalidade, constituindo-se "em um desdobramento do direito à privacidade" (Ruaro, 2015, p. 43).

Nas palavras de Mendes (2018, p. 191) "pode-se observar que o direito à autodeterminação informativa se encontra em uma relação de continuidade com a concepção do direito geral da personalidade" e que "Já existe uma rica experiência institucional em curso, há mais de duas décadas, que reconhece a evolução do conceito de privacidade, de modo a abarcar a proteção dos dados pessoais do cidadão no nosso ordenamento jurídico" (Mendes,

2018, p. 201), mas não somente isso, trata-se, segundo Poscher (2017, p. 133) em "um aprimoramento modal sistemático" dos direitos fundamentais, protegendo-os não somente dos danos concretos, reais, mas também dos abstratos e potenciais.

De acordo com o problema de pesquisa enunciado, o objetivo principal da pesquisa foi analisar, comparativamente, decisões do STF e do TCF acerca da liberdade de expressão na internet e a proteção dos direitos da personalidade.

Para cumprir o objetivo proposto, a técnica utilizada consistiu em pesquisa no site do Supremo Tribunal Federal e do Tribunal Constitucional Federal da Alemanha das ações relacionadas com a temática liberdade de expressão na internet e proteção dos direitos da personalidade *online*.

O recorte temporal da pesquisa, em relação ao STF, foi a partir de 2014, ano da entrada em vigor da lei brasileira nº 12.965, de 23 de abril de 2014, conhecida como marco civil da internet, com marco temporal final o ano de 2024, ano inicialmente previsto para o encerramento do projeto de pesquisa. Enquanto, em relação ao TCF, o prazo estipulado foi mais abrangente, a partir de 1995, considerando, dentre outras variáveis: o baixo número de julgados daquela Corte, em comparação ao STF; o fato de até o momento da propositura do projeto inexistir decisão sobre a liberdade de expressão *on-line* do TCF; e o fato de que, no ano de 1995, foi decidido o caso "os soldados são assassinos", paradigma acerca da liberdade de expressão no ambiente *off-line*[3].

A pesquisa empírica foi realizada no portal do Supremo Tribunal Federal onde há um sistema de pesquisa de jurisprudência através de palavras-chave http://www.stf.jus.br /portal/jurisprudencia/pesquisarJurisprudencia.asp, bem como no portal do TCF (https://www.bundesverfassungsgericht.de/ SiteGlobals/Forms/Suche/EN/Entscheidungensuche_Formular.ht ml?nn=5403310&submit=send&dateAfter=yyyy.MM.dd&facetted

[3] https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/19 95/10/rs19951010_1bvr147691.html

Year=2014&templateQueryString=%22Right+to+Information%22&dateBefore=yyyy.MM.dd).

Com a realização da pesquisa empírica, chegou-se ao seguinte resultado, conforme quadros abaixo:

**Quadro 1 –** Ações no Supremo Tribunal Federal pertinentes à temática da pesquisa localizadas no site do STF

| |
|---|
| **Ação/Processo:** ADI 6991, de 06/09/2021 (julgada em conjunto com as ADIs 6992, 6993, 6994, 6995,6996 e 6998)<br>**Patrocinador/Partes**: Partido Socialista Brasileiro<br>**Objeto/Tema**: Medida Provisória 1.068/2021 que objetivava alterar o Marco Civil da Internet e Lei de Direitos Autorais/Regulação das plataformas digitais<br>**Relator**: Rosa Weber |
| **Ação/Processo:** ADPF 722, de **27/07/2020**<br>**Patrocinador/Partes**: Rede Sustentabilidade<br>**Objeto/Tema**: Dossiê Antifascista<br>**Relator**: Cármen Lúcia |
| **Ação/Processo: PET 9068, de 10/08/2020**<br>**Patrocinador/Partes**: Deltan Martinazzo Dallagnol<br>**Objeto/Tema**: Manifestações no twitter<br>**Relator**: Nunes Marques |
| **Ação/Processo:** ADPF 572, 23/03/2019<br>**Patrocinador/Partes**: Rede Sustentabilidade<br>**Objeto/Tema**: Inquérito das Fake News<br>**Relator**: Edson Fachin |
| **Ação/Processo:** AP 1046, 23/06/2021<br>**Patrocinador/Partes**: Ministério Público Federal<br>**Objeto/Tema**: Daniel Lúcio da Silveira<br>**Relator**: Alexandre de Moraes |
| **Ação/Processo:** RE 1057258, 27/06/2017<br>**Patrocinador/Partes**: Google Brasil Internet Ltda<br>**Objeto/Tema**: Artigo 19 do Marco Civil da Internet<br>**Relator**: Luiz Fux |

| |
|---|
| **Ação/Processo:** ADI 6387, de 20/04/2020 (julgada em conjunto com as ADIs 6649, 6529 e ADPF 695.<br>**Patrocinador/Partes**: Conselho Federal da Ordem dos Advogados do Brasil<br>**Objeto/Tema**: Compartilhamento de dados entre empresas de telefonia e IBGE<br>**Relator**: Rosa Weber |
| **Ação/Processo:** ARE 1042075, 21/04/2017<br>**Patrocinador/Partes**: Ministério Público do Estado do Rio de Janeiro<br>**Objeto/Tema**: Sigilo de dados em telefone celular<br>**Relator**: Dias Toffoli |
| **Ação/Processo:** RE 1301250<br>**Patrocinador/Partes**: Google Brasil Internet Ltda<br>**Objeto/Tema**: identificação dos IP's ou "DEVICE IDs" que tenham se utilizado do Google Busca no caso Marielle Franco<br>**Relator**: Rosa Weber |
| **Ação/Processo:** ARE 1307386, de 19/01/2021<br>**Patrocinador/Partes**: Potelo Sistemas de Informação Ltda<br>**Objeto/Tema**: Disponibilização de processos na internet sem restrição de segredo de justiça<br>**Relator**: Cármen Lúcia |
| **Ação/Processo:** RE 1037396, 29/03/2017<br>**Patrocinador/Partes**: Facebook Serviços online do Brasil LTDA.<br>**Objeto/Tema**: Artigo 19 do Marco Civil da Internet<br>**Relator**: Dias Toffoli |
| **Ação/Processo:** RE 673707, de 23/02/2012 (julgado em 17/06/2015)<br>**Patrocinador/Partes**: Rigliminas Distribuidora Ltda<br>**Objeto/Tema**: Habeas data em relação ao Sistema de Conta Corrente da *Receita Federal* - SINCOR<br>**Relator**: Luiz Fux |

Fonte: elaborado pelo coordenador com base na pesquisa realizada no site do STF.

**Quadro 2 –** Ações no Tribunal Constitucional Federal da Alemanha pertinentes à temática da pesquisa localizadas no site do TCFA

| |
|---|
| **Ação/Processo:** 1 BvR 3214, 10 de novembro de 2020<br>**Patrocinador/Partes**: Anonimizado<br>**Objeto/Tema**: Ato de Arquivo Anti-Terrorismo II – compartilhamento de dados<br>**Órgão julgador**: Primeiro Senado |
| **Ação/Processo:** 1 BvR 1842/08; 1 BvR 6/09; 1 BvR 2538/08<br>**Patrocinador/Partes**: Anonimizados<br>**Objeto/Tema**: Colunismo social – divulgação de fotos e informações sobre celebridades<br>**Órgão julgador**: Primeiro Senado |
| **Ação/Processo:** 1 BvR 1696/98<br>**Patrocinador/Partes**: Anonimizado<br>**Objeto/Tema**: Utilização de expressões ambíguas<br>**Órgão julgador**: Primeiro Senado |
| **Ação/Processo:** 1 BvR 1619/17<br>**Patrocinador/Partes**: Anonimizado<br>**Objeto/Tema**: Lei de Proteção Constitucional da Baviera – compartilhamento de dados<br>**Órgão julgador**: Primeiro Senado |
| **Ação/Processo:** 1 BvR 1215/07<br>**Patrocinador/Partes**: Anonimizado<br>**Objeto/Tema**: Base de dados antiterrorista<br>**Órgão julgador**: Primeiro Senado |
| **Ação/Processo:** 1BvR 1073/20<br>**Patrocinador/Partes**: Anonimizado<br>**Objeto/Tema**: Liberdade de expressão e agente político, uso de expressões ambíguas<br>**Órgão julgador**: Primeiro Senado |
| **Ação/Processo:** 1BvR 1072/01<br>**Patrocinador/Partes**: Junge Freiheit GmbH&Co<br>**Objeto/Tema**: Liberdade de expressão – jornal de extrema direita<br>**Órgão julgador**: Primeiro Senado |
| **Ação/Processo:** 1BvR 370/07; 1 BvR 595/07<br>**Patrocinador/Partes**: Anonimizado<br>**Objeto/Tema**: Compartilhamento de dados<br>**Órgão julgador**: Primeiro Senado |

| |
|---|
| **Ação/Processo:** 1 BvR 276/17<br>**Patrocinador/Partes**: Anonimizado<br>**Objeto/Tema**: Direito ao esquecimento II<br>**Órgão julgador**: Primeiro Senado |
| **Ação/Processo:** 1 BvR 256, 263, 586/08<br>**Patrocinador/Partes**: Anonimizado<br>**Objeto/Tema**: Proteção de dados<br>**Órgão julgador**: Primeiro Senado |
| **Ação/Processo:** 1 BvR 16/13<br>**Patrocinador/Partes**: Anonimizado<br>**Objeto/Tema**: Direito ao esquecimento I<br>**Órgão julgador**: Primeiro Senado |
| **Ação/Processo:** 1 BvQ 42/19<br>**Patrocinador/Partes**: Anonimizado<br>**Objeto/Tema**: Exclusão de texto de partido de direita do Facebook<br>**Órgão julgador**: Primeiro Senado |
| **Ação/Processo:** 1 BvQ 22/01<br>**Patrocinador/Partes**: Anonimizado<br>**Objeto/Tema**: Reunião da direita radical<br>**Órgão julgador**: Primeiro Senado |

Fonte: elaborado pelo coordenador com base na pesquisa realizada no site do TCFA.

Com a seleção dos casos e após análise preliminar dos mesmos, esses casos foram divididos em dois grandes eixos temáticos, a saber: 1 – limites à liberdade de expressão e 2 – proteção de dados. As ações que compõem cada um desses eixos estão indicadas nos quadros que seguem:

**Quadro 3 –** Ações que compõem o eixo temático limites à liberdade de expressão

| **AÇÃO** | **TEMA** |
|---|---|
| ADI 6991 | Regulação das plataformas digitais |
| ADPF 722 | Dossiê Antifascista |

| | |
|---|---|
| PET 9068 | Manifestações no twitter |
| ADPF 572 | Inquérito das Fake News |
| AP 1044 | Daniel Lúcio da Silveira |
| RE 1057258 | Artigo 19 do Marco Civil da Internet |
| RE 1037396 | Artigo 19 do Marco Civil da Internet |
| 1 BvR 1842/08 | Colunismo social |
| 1 BvR 1696/98 | Utilização de expressões ambíguas |
| 1 BvR 1073/20 | Liberdade de expressão e agente político |
| 1 BvR 1072/01 | Jornal de extrema direita |
| 1 BvR 276/17 | Direito ao esquecimento |
| 1 BvR 16/13 | Direito ao esquecimento |
| 1 BvQ 42/19 | Partido de direita do Facebook |
| 1 BvQ 22/01 | Reunião da direita radical |

Fonte: elaborado pelo coordenador com base nas pesquisas realizadas nos sites do STF e TCF

**Quadro 4 –** Ações que compõem o eixo temático proteção de dados

| **AÇÃO** | **TEMA** |
|---|---|
| ADI 6387 | Compartilhamento de dados |
| ARE 1042075 | Sigilo de dados em telefone celular |
| RE 1301250 | Identificação de IPs e Device IDs |
| ARE 1307386 | Disponibilização de processos na internet |
| RE 673707 | Habeas data |

| | |
|---|---|
| 1 BvR 3214 | Antiterrorismo |
| 1 BvR 1619/17 | Lei de proteção da Baviera |
| 1 BvR 1215/07 | Base de dados antiterrorismo |
| 1 BvR 370/07 | Direito ao esquecimento |
| 1 BvR 256/08 | Proteção de dados |

Fonte: elaborado pelo coordenador com base nas pesquisas realizadas nos sites do STF e TCF

Feita essa divisão por eixos, a análise foi realizada em duas etapas. Em uma primeira fase (2022 e 2023), foram analisadas as ações relacionadas ao eixo limites à liberdade de expressão, tema objeto do e-book "**Limites à liberdade de expressão nas Cortes Constitucionais: pontos de convergência e divergência nos Tribunais Constitucionais brasileiro e alemão"**, publicado em novembro de 2024 e disponível em: https://s3.eu-north-1.amazonaws.com/qrlogo.io/pdf/hqdi4wwvh.pdf.

Este e-book apresenta e analisa as decisões relacionadas ao eixo proteção de dados, análises realizadas durante o ano de 2024, nas reuniões do Grupo de Pesquisa.

O eixo proteção de dados foi subdividido em 5sub-eixos: 1 – compartilhamento de dados; 2 – investigação criminal; 3 - divulgação de processos; 4 - banco de dados e 5 – proteção de dados.

**Quadro 5 –** Ações e respectivos subeixos temáticos – proteção de dados

| **AÇÕES** | **SUB-EIXOS** |
|---|---|
| ADI 6387; 1 BvR 370/07; 1 BvR 3214; 1 BvR 1619/17; 1 BvR 1215/07 | Compartilhamento de dados |
| ARE 1042075; RE 1301250 | Investigação criminal |

| | |
|---|---|
| ARE 1307386 | Divulgação de processos |
| RE 673707 | Banco de dados |
| 1 BvR 256/08 | Proteção de dados |

Fonte: elaborado pelo coordenador com base nas pesquisas realizadas nos sites do STF e TCF

Para a análise do objetivo específico da pesquisa, o método utilizado foi o indutivo. A pesquisa utilizou de técnica que consistiu na leitura minuciosa dos acórdãos/decisões proferidas pelas Cortes, analisando-se, no caso do STF, a ementa, o relatório de cada ação, os votos proferidos pelos Ministros relatores, e os votos divergentes, caso existentes. Essa opção metodológica se justifica pois considera-se, de acordo com Silva, V. (2013, p. 568), que esses documentos – em especial, ementa e acórdão - expressam "os únicos dois produtos coletivos do processo de decisão" do Supremo.

No entanto, é importante frisar que não se desconsidera aqui e também não se desconhece que essa opção de análise não é imune de críticas e questionamentos quanto ao recorte efetuado. Alguns trabalhos contestam essa opção, tais como Silva, V. (2015, 2016) e Costa (2014), contudo, outros seguem essa linha, como é o caso de Almeida e Bogossian (2016). Também não se desconsidera que o processo decisório do STF é caracterizado pelo julgamento em série, com apresentação dos votos dos Ministros em separado, conforme Klafke e Pretzel (2014) e Silva, V. (2013). Contudo, como dito e com Silva, V. (2013), ementa e acórdão são os documentos coletivos da corte.

Ademais, reconhece-se aqui também que ao relator são atribuídas inúmeras funções decisórias, como por exemplo: ordenar e dirigir o processo, submeter questões de ordem ao plenário, determinar as medidas em caráter de urgência, com apreciação *ad referendum* do colegiado, pedir dia para julgamento dos processos quando já tiver proferido o seu voto. Ainda pode

arquivar ou negar recurso intempestivo, incabível ou que contraria jurisprudência do tribunal, dentre outras funções.

Sobre o papel dos relatores no âmbito congressual, Souza (2003, p. 43) menciona que os ocupantes dessa função exercem um

> papel importante nos processos decisórios na medida que influem sobremaneira na elaboração dos anteprojetos encaminhados à votação. Como centralizadores de todas as informações disponíveis no âmbito de sua atuação formal, os relatores dispõem de um amplo raio de intervenção no que se refere ao conteúdo mesmo das proposições contidas em seus pareceres. (Souza, 2003, p. 43).

Essa constatação pode ser feita também no âmbito judicial, onde o relator de um processo exerce uma função privilegiada em relação aos demais membros julgadores, concentrando em suas mãos grandes poderes, "isso porque é ele quem escreve o relatório distribuído para os outros Ministros tomarem conhecimento do caso, sendo dele a primeira opinião a ser manifestada sobre o assunto." (Oliveira, 2006, p. 87).

Muito embora uma especial atenção será dada ao posicionamento do relator, também serão analisados os votos divergentes dos demais Ministros, caso existam, e se necessário, os votos de todos os Ministros.

Em relação aos julgados do TCF a mesma técnica será aplicada, com as devidas adaptações necessárias, considerando que o formato dos julgamentos é diferente no TCA, não há voto, somente a opinião da corte e, às vezes, com a divulgação da opinião divergente. Tendo em vista a complexidade dos casos decididos pelo TCF, foram ainda aplicados filtros adicionais: em princípio, foram excluídas as decisões de órgãos fracionários (Câmaras), privilegiando aquelas decididas por um dos Senados, que compõem o Tribunal. Nos casos do TCF, são analisados 1) o dispositivo da decisão (*Leitsatz*), 2) a situação que ocasionou a demanda, enfim, 3) os fundamentos da decisão (*Gründe*), excluídos,

neste caso, os aspectos processuais tratados na decisão (admissibilidade, legitimidade ativa, entre outros).

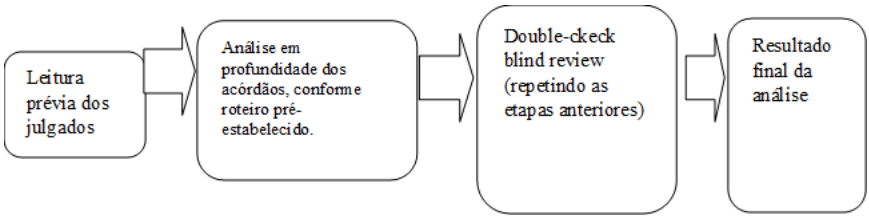
A análise dos julgados seguiu um questionário previamente definido, criando-se critérios objetivos e que potencialmente minimizam o subjetivismo da análise, o que é próprio de pesquisa de análise jurisprudencial. O questionário está indicado na sequência:

**Questionário / Roteiro para a análise dos casos**

| |
|---|
| 1 - Qual o pedido feito na ação? Ou seja, quais foram os elementos fáticos e legais? Quem propôs a ação? |
| 2 - Qual a efetiva decisão da Corte? A Corte (STF/TCF) privilegia a liberdade de expressão ou os direitos da personalidade? |
| 3 - As Cortes utilizam o princípio ou critério da proporcionalidade como método de solução dos conflitos entre a liberdade de expressão e os direitos de personalidade na rede? |

Também no intuito de minimizar o subjetivismo inerente a esse tipo de análise, a pesquisa realizou uma segunda análise, em uma espécie de *double-check blind review* em ações analisadas pelo pesquisador responsável. Esse cotejo duplo é executado pelos pesquisadores associados, em cooperação. Os alunos de graduação e pós-graduação e os membros do grupo de pesquisa colaboraram, em especial, no relato dos elementos fáticos de cada ação, como também auxiliaram na análise final dos casos.

A análise propriamente dita seguiu o seguinte roteiro/fluxograma:




A técnica de pesquisa proposta se aproxima ao que foi mencionado por Canotilho (2003, p. 1120) como método de trabalho *briefing a case*, pois serão contextualizados os casos, analisados os textos e os significados das normas, apresentadas as controvérsias, os argumentos, a retórica argumentativa, e, por fim, as decisões do STF/TCF.

A metodologia de trabalho está alinhada ao que foi definido por Bucci (2013) como "família de casos" ou "casotecas".

Trata-se, portanto, de "um exercício de Dogmática da Decisão, mediante análise crítica de algumas decisões recentes do Supremo Tribunal Federal". (Ramos, 2015, p. 30) e também do TCF.

É ainda salutar ressaltar que trabalhos e pesquisas jurídicas invariavelmente não fazem um recorte específico em relação às decisões jurisprudenciais a serem analisadas, utilizam-se costumeiramente de casos esparsos e isolados.

A pesquisa, diante disso, objetivou sistematizar as decisões do STF/TCF relacionadas à liberdade de expressão na internet e proteção dos direitos da personalidade *online*, esperando contribuir, desta forma, com a produção e divulgação do conhecimento científico, o que se faz agora neste e-book divulgando-se os resultados da pesquisa relacionados ao eixo proteção de dados.

## Referências

ALMEIDA, D. dos S; BOGOSSIAN, A. M. "Nos termos do voto do relator": considerações acerca da fundamentação coletiva nos acórdãos do STF. **Revista Estudos Institucionais**, Rio de Janeiro, v. 2, n. 1, p. 263-297, 2016.

BUCCI, M. P. D. **Fundamentos para uma teoria jurídica das políticas públicas**. São Paulo: Saraiva, 2013.

CANOTILHO, J. J. G. **Direito constitucional e teoria da constituição**. 7 ed. Coimbra: Almedina, 2003.

COSTA, T. M. da. Conteúdo e alcance da decisão do STF sobre a lei de imprensa na ADPF 130. **Revista de Direito GV**, São Paulo, n. 10(1), p. 119-154, 2014.

FARIAS, E. **Liberdade de expressão e comunicação: teoria e proteção constitucional**. São Paulo: Revista dos Tribunais, 2004.

FERREIRA, A. **Direito à informação, direito à comunicação: direitos fundamentais na Constituição Brasileira**. São Paulo: Celso Bastos Editor: Instituto Brasileiro de Direito Constitucional, 1997.

FISS, O. M. **A ironia da liberdade de expressão: estado, regulação e diversidade na esfera pública.** Rio de Janeiro: Renovar, 2005.

KLAFKE, G. F; PRETZEL, B. R. Processo decisório no Supremo Tribunal Federal: aprofundando o diagnóstico das onze ilhas. **Revista de Estudos Empíricos em Direito,** vol. 1, n. 1, p. 89-104, 2017.

MACHADO, J. E. M. **Liberdade de expressão: dimensões constitucionais da esfera pública no sistema social**. Coimbra: Coimbra Editora, 2002.

MENDES, L. S. F. Habeas data e autodeterminação informativa: os dois lados da mesma moeda. **Direitos Fundamentais & Justiça**, Belo Horizonte, ano 12, n. 39, p. 185-216, jul./dez. 2018.

NAPOLITANO, C. J.; STROPPA, T. O Supremo Tribunal Federal e o discurso de ódio nas redes sociais: exercício de direito versus limites à liberdade de expressão. **Revista Brasileira de Políticas Públicas**, v. 7, n. 3, p. 313-332, 2018.

NITRINI, R. V. Liberdade de informação e proteção ao sigilo da fonte: desafios constitucionais na era da informação digital. **Dissertação**. Universidade de São Paulo, São Paulo, 2013.

OLIVEIRA, V. E. Judiciário e privatizações no Brasil: existe uma judicialização da política. **Dados**, Rio de Janeiro, v. 48, n. 3, p. 559-587, 2005.

POSCHER, R. The right to data protection. In: MILLER, R. **Privacy and power: a transatlantic dialogue in the shadow of the NSA-Affair**. Cambridge: Cambridge University Press, 2017, pp. 129-142.

RAMOS, E. da S. **Ativismo judicial: parâmetros dogmáticos**. 2 ed. São Paulo: Saraiva, 2015.

REALE JUNIOR, M. Limites à liberdade de expressão. **Espaço Jurídico**, Joaçaba, v. 11, n. 2, p. 374-401, jul./dez. 2010.

RUARO, R. L. Privacidade e autodeterminação informativa obstáculos ao estado de vigilância? **Arquivo Jurídico**, v. 2, n. 1, p. 41-60, Jan./Jun. de 2015.

SARMENTO, D. Liberdade de expressão, pluralismo e o papel promocional do Estado**. Revista Diálogo Jurídico,** Salvador, nº. 16, 2007. Disponível no site: http://www.direitopublico.com.br.

SILVA, J. C. C. B. Democracia e liberdade de expressão. Contribuições para uma interpretação política da liberdade de palavra**. Tese**. Universidade de São Paulo, Faculdade de Filosofia, Letras e Ciências Humanas, São Paulo, 2009.

SILVA, V. A. da. **Direitos fundamentais: conteúdo essencial, restrições e eficácia**. São Paulo: Malheiros, 2009.

_____. Deciding without deliberation. **IJCL**, v. 11, n. 3, 557-584, 2013.

_____. Um voto qualquer? O papel do ministro relator na deliberação no Supremo Tribunal Federal. **Revista de Estudos Institucionais**, Rio de Janeiro, v. 1, 1, p. 180-200, 2015.

_____. O relator dá voz ao STF? **Revista de Estudos Institucionais**, Rio de Janeiro, v. 2, 2, p. 648-669, 2016.

SOUZA, M. T. O processo decisório na constituição de 1988: práticas institucionais. **Lua Nova**, São Paulo, n. 58, p. 37-60, 2003.

SUNSTEIN, C. R. **Democracy and the problem of free speech**. The Free Press: New York, 1995.

TAVEIRA, C. de O. Democracia e Pluralismo na Esfera Comunicativa: Uma Proposta de Reformulação do Papel do Estado na Garantia da Liberdade de Expressão. **Tese.** Universidade do Estado do Rio de Janeiro, Faculdade de Direito, Rio de Janeiro, 2010.

# Apresentação

Enrico Lentini Gibotti
Lucas Catib de Laurentiis
Sarah Thiemy Kawato dos Santos

Este Ebook é o resultado de uma ideia e um trabalho conjuntos. Por isso, embora composto de histórias individuais de cada um de seus autores, ele também dispõe de uma dimensão coletiva que une todos os trabalhos aqui publicados. Pelo aspecto institucional, sua concepção nasceu do Projeto de pesquisa aprovado pelo CNPq para a chamada Universal de Grupos emergentes, na qual o projeto elaborado pelos Professores Carlo Napolitano, Lucas De Laurentiis e Tatiana Stroppa foi contemplado. Porém, a realização desta obra só pôde nascer graças aos encontros realizados no Grupo de Pesquisa Mídia e Sociedade, que não só renderam debates ricos, e muitas vezes acalorados, a respeito dos julgamentos e temas que o leitor encontrará aqui.

Em geral, esses debates eram mensais e se voltaram para a discussão de decisões do Supremo Tribunal Federal e do Tribunal Constitucional Alemão, que formam os eixos do projeto aprovado pelo CNPq. Inicialmente, foi dedicado a temas relacionados à liberdade de expressão, especialmente o PL das Fake News (PL 2630), mas cujo escopo foi ampliando-se na medida em que os debates foram se intensificando. Em pleno século XXI, o grupo não pode se esquivar de discutir sobre temas recorrentes e, em certa medida, desafiadores, como o advento da internet e suas diversas possibilidades de uso. Como fruto daqueles encontros, foi elaborado o primeiro ebook, sobre a temática da liberdade de expressão em uma interface entre os Tribunais Constitucionais brasileiro e alemão.

Diante do exitoso trabalho em conjunto desenvolvido naquela ocasião, o grupo se predispôs a desenvolver um segundo ebook, agora com enfoque no tema mais recentemente debatido nos encontros mensais, a proteção de dados e a privacidade nas mesmas Cortes Constitucionais.

Desde a coleta massiva de informações, frequentemente efetivada sem o consentimento adequado ou o devido tratamento dos dados coletados, que se intensificam na medida em que as tecnologias possibilitam um controle cada vez maior da vida privada dos indivíduos, até as medidas jurídicas adotadas para a prevenção do terrorismo em sociedades submetidas a intensa vigilância, o leitor pode encontrar ao longo deste ebook, que muito discute acerca dos dilemas que emergem na tentativa de equilibrar a garantia das liberdades individuais e valores fundamentais de um Estado de Direito, como a segurança pública. Em muitos casos, a falta de clareza nas legislações e as diversas interpretações jurídicas possíveis trazem maiores desafios para a identificação de caminhos viáveis e soluções jurídicas.

É oportuno frisar que o Grupo é composto por pesquisadores de diversos níveis de formação (graduandos que desenvolvem projeto de iniciação científica, mestrandos, mestres, doutorandos e doutores) e de distintas áreas, advogados (Direito) e jornalistas (Comunicação Social). Embora as decisões do STF e do TCA sejam objetos de análise que possuem maior proximidade com o cotidiano de juristas, os pesquisadores da Comunicação Social também atuaram com protagonismo na elaboração deste ebook, e é isto que o torna enriquecedor e plural. Por essa razão, os olhares para os casos estudados também são distintos e complementares. Ao longo das subdivisões do Grupo para a análise de cada caso foi empenhado um esforço para unir pesquisadores de ambas as áreas e de graus de formação diversos, justamente para que os autores pudessem desenvolver suas habilidades de pesquisa em equipe e para que a contribuição específica de cada um enriquecesse a pesquisa e proporcionasse uma abordagem mais ampla e interdisciplinar de cada tema em questão.

A ideia possuía características que apontavam para a criação de uma obra que não só descrevesse as peculiaridades dos direitos pesquisados (proteção de dados e privacidade), tal qual vistos pelos Tribunais, mas que também pudesse indicar aos comunicadores sociais o caminho que leva à efetivação desses mesmos direitos. Pode parecer simples, mas o trabalho de simplificação de julgados complexos, como os que foram tematizados aqui, não é nada simples. Este é um trabalho de conjugação de olhares e pontos de vista, por meio do qual tentamos pensar como o outro vê o argumento técnico-jurídico, que na linguagem dos tribunais é ornamentada por ares de hermeticidade e pompa. Em sentido inverso, buscamos aqui fazer uma dupla mudança de paradigma. Primeiro porque aqui aqueles que trabalham e atuam com o objeto pesquisado (a proteção de dados) se coloquem no lugar de leitores dos argumentos jurídicos que tratam da realidade que lhes é mais comum e presente; segundo porque colocamos os juristas em pé de igualdade com os demais interlocutores, retirando deles o pedigree de detentores da chave do melhor argumento, até que se prove o contrário. É verdade que os trabalhos que compõem esta obra não são, nem pretendem ser obras clássicas sobre a matéria. São relatos de fatos, relatos de situações e relatos de pessoas reais. Aqui o leitor não encontrará grandes teorias, grandes ideologias ou grandes propostas de solução. Não apresentamos Deuses do olimpo, Juízes hercúleos ou teorias revolucionárias. Nada comparado às histórias de uma Ilíada, ou Eneida. Mas algo muito próximo do que vemos na nossa vida quotidiana.

Com a proposta do trabalho em mente, os autores iniciaram as atividades. Do início ao término de sua confecção os mais diversos esforços foram empregados: da separação de temas relevantes a serem identificados nas decisões selecionadas até mesmo o processo de colheita das respectivas sentenças, cada uma das peças foi sendo cuidadosamente alocada por aqueles que se dispuseram a contribuir com a obra.

O próprio processo de elaboração do material foi em si elucidativo em diversas questões que foram mais profundamente exploradas no corpo dos relatos em si. Dos casos selecionados, embora seja possível observar uma confluência de problemas, as particularidades existem e se intensificam, principalmente levando em consideração particularidades factuais de cada Corte. O Tribunal Constitucional Federal Alemão, por exemplo, muito lidou com coleta de dados e sua subsequente partilha com outros órgãos de segurança. O comportamento é justificado pelo temor de ataques terroristas que haviam recentemente ocorrido, não só na Alemanha, mas na Europa como um todo, e encontrava fundamento legal em leis de proteção do Estado Alemão. Esse cenário justificou, não tão raramente, que procedimentos invasivos e violadores de direitos fossem autorizados por certos diplomas legais. A partir disso o Tribunal trabalha então a relação existente entre a proteção do Estado com a violação de determinados direitos em consequência deste fim almejado.

O Supremo Tribunal Federal, embora não necessariamente trate de "terroristas", como ocorre com o Tribunal Constitucional Federal Alemão, lida com questões principiológicas e técnicas sobre essa nova matéria que vem sendo regulada, ou menos a tentativa de assim fazê-lo. A elaboração, por exemplo, de medidas provisórias que violem direitos de intimidade, honra e até mesmo a vida privada das pessoas são plenamente passíveis de serem impugnadas perante o pretório excelso, como assim já foram. Mais de uma vez o Supremo Tribunal Federal, inclusive, reconheceu a proteção de dados pessoais como sendo um direito fundamental autônomo o que gerou, posteriormente, sua elevação ao patamar de direito fundamental expresso na Constituição.

De toda forma, os relatos buscam situações variadas a serem apresentadas. Os mais diversos cenários são retratados e cada qual com sua peculiaridade, contudo, guardando respeito à proposta com a qual o trabalho dialoga e oferecendo algumas ideias que o leitor pode, eventualmente, ruminar. Seria desonestidade dos autores não assumir que parte da relevância da presente obra está

em levar até os leitores que orbitem diferentes esferas sociais, profissionais e acadêmicas, questionamentos simples em questões que não parecem ser, mas na verdade são extremamente impactantes.

Com o trabalho realizado resta a parte mais importante, tal qual, a leitura por aqueles que, de uma forma ou outra, entendem que existe algum valor em discutir assuntos cujas molduras legais, e até mesmo morais, ainda estejam sendo erigidas. A pretensão da obra não recai em oferecer um caminho a ser seguido. Não. Em termos mais honestos, os autores se propõem a demonstrar como os problemas enfrentados nos casos selecionados são lidados por órgãos de cúpula que, por bem ou por mal, provocam alterações substanciais nas vidas de todos.

Nessa toada, em que pese a abordagem mais pragmática do que dogmática adotada ao longo do desenvolvimento da obra, espera-se que este ebook de alguma forma e em alguma medida contribua para a difusão do conhecimento prático quanto às problemáticas sociais e jurídicas envolvendo a proteção de dados, a privacidade e os temas correlatos. Fora isso, também se espera sobretudo que o conteúdo ora desenvolvido encoraje aqueles que se dispuserem à leitura a desenvolver novos debates e novas pesquisas acadêmicas envolvendo os problemas tão atuais e de complexa solução que rapidamente foram debatidos ao longo deste trabalho.

# EIXO COMPARTILHAMENTO DE DADOS

# Protegendo o Estado de movimentos terroristas: qual é o limite?

Enrico Lentini Gibotti
Samara Meneses Brito

## Introdução

Este trabalho tem como objetivo analisar como o Tribunal Constitucional Federal da Alemanha (TCF) tratou de questões relacionadas à segurança nacional e direitos fundamentais no combate ao terrorismo, especialmente no que tange à vigilância, processamento de dados e proteção da privacidade. Para tanto, serão analisados quatro casos específicos: BvR 370/07, BvR 1215/07, BvR 3214/15 e BvR 1619/17. O debate central nessas ações envolve a necessidade de equilibrar a segurança do Estado contra ameaças terroristas com a proteção de direitos como a privacidade e a autodeterminação informativa. O dilema consiste em, de um lado, a necessidade de fortalecer o aparato estatal para prevenir ataques terroristas e, de outro, garantir que essas medidas de proteção não infrinjam os direitos básicos dos cidadãos. O artigo se propõe a examinar cada um desses casos com base em perguntas fundamentais: quais foram os pedidos das ações? Quem propôs as ações? Quais os elementos fáticos e legais? E qual foi a decisão final do tribunal? A partir dessas respostas, será possível verificar se o Tribunal priorizou a segurança nacional, a proteção dos direitos fundamentais, ou um equilíbrio entre ambos, além de examinar os argumentos que sustentaram as decisões.

Este texto está organizado da seguinte forma: primeiramente, é apresentado um panorama sobre as ameaças terroristas na Alemanha ao longo dos anos, enfatizando sua conexão com o monitoramento online e a proteção de dados, que são conceitos

essenciais para a análise. Na sequência, cada um dos quatro processos é detalhado separadamente. Por fim, são apontadas considerações finais a respeito do material averiguado.

**Ameaças terroristas na estrutura de segurança da Alemanha**

Após os atentados de 11 de setembro de 2001 nos Estados Unidos e 11 de março de 2004 em Madrid, os países da União Europeia começaram a criar planos estratégicos de longo prazo para combater o terrorismo. Esses planos têm como principais objetivos: prevenir e combater as causas do terrorismo, proteger a população e reduzir sua vulnerabilidade, identificar e investigar atos terroristas com antecedência, e, por fim, melhorar a resposta em caso de um ataque terrorista.

Na Alemanha os debates sobre os direitos fundamentais e o combate ao terrorismo é influenciado por eventos significativos, que impulsionaram a implementação de medidas mais severas de vigilância e controle estatal. Esses episódios moldaram o cenário jurídico e deram origem a decisões importantes do Tribunal Constitucional Federal (TCF), especialmente no que diz respeito à proteção de dados pessoais e à privacidade.

Em 2019, na cidade de Halle, um extremista atacou uma sinagoga onde 52 judeus estavam rezando e tentou realizar um massacre. Ele conseguiu matar duas pessoas e transmitiu suas ações ao vivo na internet, tornando-se um dos casos mais graves do país desde o final da Segunda Guerra Mundial. O ocorrido reacendeu as discussões sobre vigilância preventiva e a responsabilidade do Estado em monitorar organizações antissemitas na internet, que se reúnem em fóruns de discussão anônimos conhecidos como "*imageboards*". A Alemanha, particularmente sensível ao crescimento do extremismo, especialmente de natureza neonazista, intensificou o monitoramento dessas organizações suspeitas com base na Lei de Proteção da Constituição. Horst Seehofer, ex-ministro do Interior da Alemanha, tomou medidas para proibir o grupo extremista "*Combat 18 Deutschland*" em 2020, que se autodenominava como uma

organização de combatentes de Adolf Hitler. Com a proibição, o uso do logotipo e da inscrição do grupo tornou-se punível por lei. Na época, as autoridades de segurança alemãs estimavam que o grupo neonazista contava com cerca de 20 membros, que supostamente se comprometeram a manter uma rigorosa confidencialidade entre si. O lema dos neonazistas, "*Whatever it takes*" (o que for necessário), refletia sua disposição para ações extremas.

O assassinato do político da CDU de Kassel, Walter Lübcke, em junho de 2019, gerou uma pressão significativa entre os ministros do interior estaduais pela dissolução do "*Combat 18*". O assassino de Lübcke, Stephan Ernst, tinha, pelo menos no passado, contato com apoiadores do grupo. Além disso, a Europol, a agência de polícia da União Europeia, também emitiu alertas sobre as atividades transfronteiriças do "Combat 18", indicando a extensão e a gravidade do extremismo associado a essa organização.

Esses exemplos mostram como eventos de alta repercussão na Alemanha afetaram diretamente o rumo das decisões judiciais, especialmente em casos envolvendo a proteção de direitos fundamentais em face de políticas de segurança cada vez mais restritivas. A análise dessas interações é fundamental para entender o delicado equilíbrio entre segurança e direitos civis em um contexto de crescente organizações terroristas.

**BvR 370/07**

Dentro do escopo de decisões trazidas para comento a BvR 370/07, julgada em conjunto com a BvR 596/07, indica o início da preocupação do Estado alemão com a utilização da internet para fins que ameacem a segurança pública. A reclamação constitucional almeja discutir a constitucionalidade do parágrafo 5(2) nº 11 da Lei de Proteção da Constituição da Renânia do Norte-Vestefália, uma vez que o referido dispositivo seria incompatível com o Artigo 2(1), em conjunto com o Artigo 1(1), Artigo 10(1) e Artigo 19(1), segunda parte, todos da Lei Básica.

A referida lei discrimina os poderes do *Land Office* com a finalidade de proteger a Constituição. É indicado que tal proteção, no caso, pode ser realizada através da coleta de dados contidos em sistemas de tecnologia e, em um segundo momento, no processamento destes dados. Ocorre que existem dois mecanismos de investigação que podem ser utilizados pelo *Land Office*. O primeiro seria, essencialmente, o monitoramento secreto a ser realizado na internet, um procedimento em que é obtido conhecimento a respeito do conteúdo das informações que trafegam pela internet através de meios técnicos ordinários (Alemanha, 2007). O segundo, por outro lado, seria o acesso encoberto a sistemas de tecnologia da informação, uma infiltração técnica que se vale, por exemplo, de vulnerabilidades do sistema de segurança ou da instalação de *spywares* com a finalidade monitoramento, obtenção de informações ali contidas ou até mesmo controle remoto do sistema alvo (Alemanha, 2007).

A justificativa conferida para tal disposição, especialmente no tocante a buscas remotas, é que existe uma necessidade de adaptação às dificuldades emergentes, no contexto de investigações criminais, em que os criminosos de grupos extremistas e terroristas utilizam os meios tecnológicos, mais especialmente a internet, para se comunicarem e ajustarem seus planejamentos com a finalidade de levar às vias de fato atos de violência. Contudo, ainda que esse novo cenário justifique a preocupação com o uso indiscriminado da internet, o TCF ainda reconheceu a inconstitucionalidade do parágrafo 5(2) nº 11 da Lei de Proteção da Constituição da Renânia do Norte-Vestefália, reconhecendo a violação de direitos fundamentais encontrados na Lei Básica. Tal conclusão decorre do reconhecimento de que tanto o requerimento da (i) clareza legal, assim como a (ii) proporcionalidade e a (iii) necessidade de mecanismos de proteção não foram respeitados (Alemanha, 2007).

A clareza legal, requerimento atrelado diretamente ao princípio do *rule of law* e que está presente nos Artigos 20 e 28(1) da Lei Básica, possibilita, entre outras finalidades, que aqueles sujeitos

a aplicação da lei tenham ciência de como a mesma é aplicada e, consequentemente, consigam discernir o permitido do não permitido a fim de tomar precauções contra medidas potencialmente invasivas. Ocorre que a disposição contestada faz diversas referências a outros artigos que não permitem, com facilidade e clareza, uma conclusão evidente e nítida daquilo que a lei se propõe a fazer. De maneira semelhante, tendo em vista o caráter invasivo das medidas ali previstas, não é possível dizer que existem mecanismos de proteção compatíveis com a salvaguarda de informações pessoais obtidas.

O TCF, então, faz menção expressa a utilização do princípio da proporcionalidade. Na medida em que o princípio exige que a interferência com os direitos fundamentais sirva um fim legítimo, bem como seja cabível, necessária e apropriada para atingir este objetivo, o dispositivo contestado falha em suprir o critério da proporcionalidade *stricto sensu* (Alemanha, 2007). Ainda que o fim seja reconhecidamente legítimo, tal qual a proteção contra *konkrete Gefahren* (perigo concreto) decorrente de grupos terroristas, e que a adequação e a necessidade dos mecanismos estejam de acordo com a finalidade indicada, o TCF indica que as medidas contidas no dispositivo contestado interferem nos direitos fundamentais de maneira tão séria que são desproporcionais, fazendo, mais uma vez, referência direta a necessidade de mecanismos de proteção como uma das razões da falha aqui indicada.

Quadro sinótico BvR 370/07

**1 - Qual o pedido feito na ação? Ou seja, quais foram os elementos fáticos e legais? Quem propôs a ação?**

O pedido feito na ação versa sobre a constitucionalidade da fiscalização da internet pelo *Land Office*, principalmente através da utilização de meios encobertos e invasivos nos sistemas alvos das investigações. Os autores da ação foram mantidos em sigilo, havendo apenas a menção às atividades por eles realizadas e que resultaram na judicialização da demanda.

| |
|---|
| **2 - Qual a efetiva decisão da Corte? A Corte (STF/TCF) privilegia a liberdade de expressão ou os direitos da personalidade?**<br>A decisão da Corte entendeu que, embora a lei disponha de um objetivo válido, tal qual a proteção do Estado contra atos terroristas, o grau de invasão permitido pelo dispositivo questionado provoca uma violação sistemática de direitos fundamentais, em especial da personalidade, que geram a inconstitucionalidade das medidas pretendidas. Há, portanto, uma prevalência dos direitos da personalidade. |
| **3 - As Cortes utilizam o princípio ou critério da proporcionalidade como método de solução dos conflitos entre a liberdade de expressão e os direitos de personalidade na rede?**<br>Sim, o critério da proporcionalidade foi utilizado. |

Fonte: quadro elaborado pelos autores.

**BvR 1215/07**

A reclamação constitucional em questão é um dos primeiros e principais contatos que o TCF tem com a Lei do Arquivo Antiterrorista, de 22 de dezembro de 2006. A legislação em questão prevê a criação de um arquivo antiterror central e padronizado a ser organizado e utilizado tanto por serviços de inteligência como por autoridades policiais no combate ao terrorismo internacional (Alemanha, 2007). Com a criação de um sistema único a pretensão é que as atividades administrativas e, quando cabível, as atividades operacionais tenham agilidade e facilidade em encontrar as informações necessárias na prevenção de atividades terroristas.

A legislação dispõe de uma série de informações a respeito de como esse banco de dados será criado, quais são as autoridades que podem ter acesso às informações ali contidas, como deve ocorrer eventual compartilhamento de dados e até mesmo procedimentos para retificação e remoção de informações. O principal elemento que deve ser considerado aqui, e que foi o questionamento levado ao TCF pelo autor (anonimizado), é referente a extensão em que pessoas afetadas pela lei devem ser notificadas. O parágrafo 2 da

Lei do Arquivo Antiterrorista indica quais são as pessoas que devem ter suas informações inseridas no sistema, as quais incluem desde pessoas diretamente investigadas por conta de seus próprios atos até aquelas que tiveram interações pontuais com essas que são objetivamente investigadas, salvo em casos que o contato tenha ocorrido de maneira breve e acidental.

Uma vez que tal requisito previsto no parágrafo 2 tenha sido atingido, o parágrafo subsequente trata de quais informações sobre essas pessoas devem ser armazenadas, havendo distinção entre dois "blocos" de informação: informação básica[4] (*Grunddaten*) e informação expandida[5] (*erweiterte Grunddaten*). Para além do fato de que tais informações podem ser compartilhadas entre autoridades, fato é que uma vez que elas são armazenadas no respectivo banco de dados, direta ou indiretamente, o indivíduo passa a ter, ainda que minimamente, um "rótulo" de potencial terrorista. Tais informações que não tenham sido armazenadas secretamente, quando requisitadas, podem ser compartilhadas com aqueles que venham a requerê-la.

O questionamento levantado é que, uma vez que, via de regra, o indivíduo que tenha sido inserido no respectivo banco de dados não tem essa informação, podendo apenas assim saber caso procure a mesma, há uma violação dos direitos fundamentais da autodeterminação, privacidade de correspondência e telecomunicação e inviolabilidade do domicílio, previstos nos Artigos 2(1), em conjunto com o Artigo 1(1), do Artigo 10(1) e do Artigo 13(1) em vinculação com o Artigo 19(4), todos da Lei Básica.

---

[4] Abrange informações como: endereço, características físicas, linguagens e dialetos falados, fotografias, bem como a(s) razão(es) que levaram ao respectivo armazenamento.

[5] Abrange informações como: dispositivos de telecomunicação que utiliza, dados bancários, origem étnica, afiliação religiosa, habilidades relevantes para atividades terroristas, informações sobre educação e treinamento, informações sobre trabalho e estruturas importantes às quais tem acesso, quão propensa é a pessoa a ser violenta e locais de visita que possam servir como ponto de encontro para pessoas suspeitas de atos terroristas.

O principal argumento que corrobora o questionamento é de que, ainda que haja uma possibilidade de retificação e até mesmo retirada de informações do banco de dados, procedimento legalmente previsto, o indivíduo não consegue ter um controle razoável de quando essas informações a seu respeito são inseridas no sistema, podendo apenas haver um controle *a posteriori* que não seria suficiente como medida de segurança tendo em vista a intensidade da ingerência verificada nos direitos fundamentais em questão.

O TCF abordou a questão através da proporcionalidade. Reconheceu tanto a necessidade quanto a adequação da lei, bem como, em abstrato a proporcionalidade *stricto sensu* das medidas ali elencadas, uma vez que elas não seriam, *per se*, desproporcionais. Ocorre que no caso elas não satisfazem a proporcionalidade *stricto sensu* por uma razão sistêmica. As medidas e procedimentos estabelecidos na lei, por mais que sejam invasivos e até mesmo detentores de grande peso probatório, poderiam ser adotados caso houvesse uma detalhada e clara especificação de como ocorrem todos os procedimentos administrativos entre as autoridades com acesso ao banco de dados central. Essa clareza não foi verificada, assim, gerando a insuficiência da proporcionalidade auferida no caso.

Quadro sinótico BvR 1215/07

| |
|---|
| **1 - Qual o pedido feito na ação? Ou seja, quais foram os elementos fáticos e legais? Quem propôs a ação?**<br>O pedido feito na ação versa sobre a constitucionalidade do procedimento de controle das informações inseridas nos bancos de dados de legislação antiterrorista. O autor da ação foi mantido em sigilo. |
| **2 - Qual a efetiva decisão da Corte? A Corte (STF/TCF) privilegia a liberdade de expressão ou os direitos da personalidade?**<br>A decisão da Corte entendeu que, embora a lei supra todas os critérios previstos pela proporcionalidade *lato sensu*, inclusive indicando que a proporcionalidade *stricto sensu* não foi *per se* violada, a falta de clareza da lei, somado ao grau de ingerência dos procedimentos sobre os direitos fundamentais, gera, em termos práticos, um resultado |

| |
|---|
| desproporcional. Assim, foram privilegiados os direitos de personalidade |
| **3 - As Cortes utilizam o princípio ou critério da proporcionalidade como método de solução dos conflitos entre a liberdade de expressão e os direitos de personalidade na rede?**<br>Sim, o critério da proporcionalidade foi utilizado. |

Fonte: quadro elaborado pelos autores.

**BvR 3214/15**

Tendo em vista o conjunto de decisões do TCF que lidam com a temática de coleta, armazenamento e até mesmo compartilhamento de dados, a BvR 3214/15, assim como a BvR 1619/17, que será brevemente comentada nas páginas seguintes, possui como plano de fundo um conjunto de ações que almejam a proteção do Estado contra atividades terroristas. A presente reclamação tem como alvo o conteúdo indicado na Seção 6.a da Lei do Arquivo Antiterrorista, de 22 de dezembro de 2006, mesma legislação discutida na BvR 1215/07.

A lei em questão tem a pretensão de sistematizar as informações coletadas em um banco de dados único que pode ser acessado pelas autoridades autorizadas para tanto. Para além da autoridade que foi responsável pela coleta dos dados em si, outras autoridades não podem ter acesso a informações que não sejam aquelas consideradas "básicas", ou seja, nome, sexo e data de nascimento de pessoas ali cadastradas. Outras informações como dados bancários, estado civil e etnia só podem ser acessadas, via de regra, pelas autoridades que foram responsáveis pela respectiva coleta das informações. Essa regra é excetuada em situações urgentes em que, para além deste acesso, é permitido uma "utilização alargada de dados". A presente reclamação impugna este aspecto em específico da Lei do Arquivo Antiterrorista.

O problema que é exposto com a possibilidade da "utilização alargada de dados" é que, com o maior acesso às informações, há a

possibilidade de conexões e cruzamento de dados entre pessoas, grupos de pessoas, instituições, objetos e coisas que habilitam a produção de novas informações e *insights* por parte das autoridades que possuem acesso aos dados (Alemanha, 2015). Tal uso estendido é indicado como sendo um caso típico de "mineração de dados", ou seja, a busca ativa por informações armazenadas nestes bancos de dados que, embora isoladas, no momento em que são cruzadas, oferecem informações totalmente novas, mas não necessariamente previstas e reguladas pela própria Lei.

A possibilidade de as pessoas terem acesso aos dados e cruzamentos realizados que lhes dizem respeito é possível e tem previsão legal, contudo, uma vez que isso só pode ser realizado posteriormente a "rotulação" de um indivíduo como potencialmente perigoso (aos olhos da lei), este fato provocaria uma ingerência indevida com certos direitos fundamentais previstos na constituição, em especial, o direito à autodeterminação informativa. Essa ingerência, aos olhos do TCF, especificamente na forma da utilização alargada, não é consistente com o princípio da proporcionalidade (Alemanha, 2015). Referida consideração é acompanhada do juízo de que tais intervenções em direitos fundamentais são necessárias quando elas perseguem um fim legítimo e um interesse público, portanto, obedecendo a adequação, a necessidade e a proporcionalidade em *stricto sensu*, o que não ocorre no presente caso.

O dispositivo legal, embora seja justificado tendo em vista o histórico de eventos de natureza terrorista vivenciada, não é suficientemente limitada e específica com relação às informações que são utilizadas pelas autoridades que têm acesso a elas. Não apenas, mas a lei prevê que tal uso expandido possa ocorrer períodos prolongados e até mesmo em situações que a urgência requerida não esteja necessariamente pautada em eventos minimamente concretos ou sequer previsíveis, ainda que improváveis. Esse conjunto de abstrações geram a conclusão de que a Seção 6.a, parágrafo 2, sentença 1, da Lei do Arquivo

Antiterrorista viola o direito fundamental à autodeterminação informativa previsto na Lei Básica.

Quadro sinótico BvR 3214/15

| |
|---|
| **1 - Qual o pedido feito na ação? Ou seja, quais foram os elementos fáticos e legais? Quem propôs a ação?**<br>O pedido feito na ação versa sobre a constitucionalidade da "utilização alargada" (mineração de dados) de bancos de dados em legislação antiterrorista. O autor da ação foi mantido em sigilo. |
| **2 - Qual a efetiva decisão da Corte? A Corte (STF/TCF) privilegia a liberdade de expressão ou os direitos da personalidade?**<br>A decisão da Corte entendeu que, embora a lei disponha de um objetivo válido, não há clareza suficiente nos procedimentos ali pretendidos, portanto, possibilitando uma ingerência desproporcional aos direitos de personalidade que, no caso, foram privilegiados. |
| **3 - As Cortes utilizam o princípio ou critério da proporcionalidade como método de solução dos conflitos entre a liberdade de expressão e os direitos de personalidade na rede?**<br>Sim, o critério da proporcionalidade foi utilizado. |

Fonte: quadro elaborado pelos autores.

**BvR 1619/17**

A reclamação constitucional BvR 1619/17 objetiva discutir sobre as disposições contidas na Lei de Proteção Constitucional da Baviera. A referida legislação tem como objetivo geral a melhora do sistema de proteção da região da Baviera, tendo em vista as disposições constitucionais do país, dada a alta ameaça e o potencial perigo decorrente do terrorismo islâmico (Alemanha, 2017). A forma encontrada para alcançar o supramencionado objetivo é a promoção da cooperação entre serviços de informações, bem como destes serviços com a própria polícia. Ocorre que os dispositivos encontrados na lei em questão dispõem de métodos variados e altamente intrusivos para a obtenção de diversas

informações a respeito daqueles que estão sendo vigiados, métodos esse que parecem sobrepujar uma série de direitos fundamentais.

Os autores da ação são, essencialmente, membros e funcionários ativos de organizações que estão sob vigilância da Lei de Proteção da Baviera que, de modo geral, questionam a constitucionalidade de diversos poderes de coleta e compartilhamento de dados previstos na legislação atacada. Em última análise, a queixa é dirigida aos poderes de vigilância ali previstos. De maneira ainda mais específica, o questionamento recai sobre a constitucionalidade de diversos termos que podem ser encontrados nos artigos da lei, exemplificativamente, termos como "vigilância de residências particulares", "buscas remotas de sistema de tecnologia da informação" e até mesmo "rastreamento de dispositivos móveis" (Alemanha, 2017).

A questão, quando perante o TCF, é inicialmente abordada com o apontamento de que não apenas as disposições impugnadas, mas a lei como um todo, permite a ingerência em direitos fundamentais. A Corte indica, especificamente, que tal ingerência recai sobre direito geral de personalidade, direito à privacidade de correspondência, correios, telecomunicações, assim como o direito à inviolabilidade do domicílio. De toda forma, em que pese a nítida interferência verificada, a Corte indica que o objetivo almejado pela legislação impugnada é legítimo, para além do fato que as próprias disposições satisfazem os requisitos da proporcionalidade[6] *lato sensu*, tais quais:

[6] Importante salientar que o critério da proporcionalidade, tal qual normalmente adotado pelo TCF, assim como em outras Cortes Constitucionais, utiliza a abordagem da proporcionalidade *lato sensu* que, por sua vez, ostenta três etapas que devem ser cumulativamente satisfeitas para que o resultado geral da verificação de proporcionalidade seja positivo. As etapas são: adequação, necessidade e proporcionalidade em sentido estrito. A adequação versa sobre a verificação da relação entre ação e resultado, ou seja, caso determinada conduta seja realizada, obter-se-á o resultado desejado? A necessidade, por sua vez, debruça-se sobre o questionamento se, ainda que a ação almejada seja adequada (na forma previamente exemplificada), é necessária, tendo em vista que outras abordagens que gerem o mesmo resultado possam existir. A proporcionalidade em sentido estrito, finalmente, busca avaliar qual das condutas que subsistiram

a adequação e a necessidade. Entretanto, peca com relação ao critério da proporcionalidade *stricto sensu* (Alemanha, 2017).

A Corte reconhece que a proteção da democracia e dos direitos fundamentais, principalmente considerando que o Estado Alemão adota o princípio da democracia militante, importa em eventuais ingerências em direitos fundamentais, o que, contudo, não deve implicar em uma violação desregrada destes direitos. Utilizando-se do critério da proporcionalidade (o que consta *ipsis litteris* na decisão), a Corte indica que o referido critério, em sua verificação *stricto sensu*, importa em diferentes limites da obtenção de informações pessoais. Uma agência de fiscalização e supervisão pode ter limites mais abrangentes quanto aos métodos disponíveis para a obtenção de informações pessoais do que o órgão de polícia, o que se dá em função da ausência dos poderes de acompanhamento operacional (*follow-up powers*) daquele. Ou seja, uma agência de inteligência não dispõe de poderes para concretizar prisões a partir de eventuais informações incriminadoras, o que não é verdade para um órgão de polícia.

Essa afirmação também gera consequências para o compartilhamento das respectivas informações. O órgão de inteligência não pode compartilhar toda e qualquer informação com os órgãos de polícia sob pena de tornar sem efeito aquilo que permite a expansão dos poderes de fiscalização da agência de inteligência, uma vez que poderia passar quaisquer dados para a polícia que então tomaria as ações concretas. De acordo com a Corte, a agência detentora de informações, antes de compartilhar os dados obtidos através de seus procedimentos próprios, precisa proceder a um "juízo hipotético de recolhimento de dados", ou seja: avaliar se dentro das próprias competências legais

---

aos dois critérios anteriores é menos danosa ao sistema jurídico, principalmente em termos de conflitos de direitos. Aquela conduta que for apta a atingir o fim almejado da forma menos danosa ao sistema, de modo geral, deve ser aquela adotada.

estabelecidas para o órgão receptor tais informações poderiam ser obtidas autonomamente obtidas por ele (Alemanha, 2017).

A Corte entende que, uma vez que não existe claridade sobre como as informações dos investigados será obtida pela agência de inteligência, sua forma de armazenamento e nem o detalhamento referente ao compartilhamento das informações obtidas, todos os termos impugnados carecem de constitucionalidade. Sob essa perspectiva, é possível dizer que o TCF dá preferência aos direitos de personalidade em detrimento aos procedimentos de defesa do Estado.

Quadro sinótico BvR 1619/17

| |
|---|
| **1 - Qual o pedido feito na ação? Ou seja, quais foram os elementos fáticos e legais? Quem propôs a ação?**<br>O pedido feito na ação versa sobre a constitucionalidade dos poderes de fiscalização e compartilhamento de dados da forma expressa na Lei de Proteção Constitucional da Baviera. A ação foi proposta por membros de órgãos sujeitos à fiscalização da lei em questão. |
| **2 - Qual a efetiva decisão da Corte? A Corte (STF/TCF) privilegia a liberdade de expressão ou os direitos da personalidade?**<br>A decisão da Corte entendeu que, embora a lei disponha de um objetivo válido, não há clareza suficiente nos procedimentos ali pretendidos, portanto, possibilitando uma ingerência desproporcional aos direitos de personalidade que, no caso, foram privilegiados. |
| **3 - As Cortes utilizam o princípio ou critério da proporcionalidade como método de solução dos conflitos entre a liberdade de expressão e os direitos de personalidade na rede?**<br>Sim, o critério da proporcionalidade foi utilizado. |

Fonte: quadro elaborado pelos autores.

## Considerações Finais

Como pôde ser observado, o Estado Alemão possui considerável aparato legal visando a sua proteção contra atos

terroristas. Vale-se, inclusive, de leis que dispõem sobre procedimentos invasivos para a mais vasta obtenção possível de informações que possam auxiliar nessa tarefa. Não parece, contudo, que tais procedimentos estejam isentos de limites, estes que são estabelecidos pelos direitos fundamentais previstos na Lei Básica. A proporcionalidade, amplamente utilizada em todos os casos aqui relatados, indicou constantemente que há uma preocupação do TCF em conter movimentos terroristas, mas também que essa empreitada não deve ser feita de maneira desregrada e sem levar em consideração os efeitos experienciados pelo cidadão comum.

## Referências


ALEMANHA, Der Spiegel. "Combat 18: Innenminister Horst Seehofer verbietet Neonazi-Gruppe." Der Spiegel, 23 de janeiro de 2020. Disponível em: https://www.spiegel.de/politik/deutschland/combat-18-innenminister-horst-seehofer-verbietet-neonazi-gruppe-a-21aaf774-9ff4-4dfd-bda6-71f6d376ed8a

ALEMANHA, Tribunal Constitucional Federal da Alemanha. **1 BvR 1215/07.** 24 de abril de 2013. Disponível em: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2013/04/rs20130424_1bvr121507en.html. Acesso em 01 out. 2024.

ALEMANHA, Tribunal Constitucional Federal da Alemanha. **1 BvR 1619/17.** 26 de abril de 2022. Disponível em: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2022/04/rs20220426_1bvr161917en.html. Acesso em 01 out. 2024.

ALEMANHA, Tribunal Constitucional Federal da Alemanha. **1 BvR 3214/15.** 10 de novembro de 2020. Disponível em: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2020/11/rs20201110_1bvr321415en.html. Acesso em 01 out. 2024.

ALEMANHA, Tribunal Constitucional Federal da Alemanha. **1 BvR 370/07.** 27 de fevereiro de 2008. Disponível em: https://www.bundesver

fassungsgericht.de/SharedDocs/Entscheidungen/EN/2008/02/rs20080227_1bvr037007en.html. Acesso em 01 out. 2024.

BRASIL, Deutsche Welle. "Autor de atentado em Halle é condenado à prisão perpétua." DW, 21 de janeiro de 2020. Disponível em: https://www.dw.com/pt-br/autor-de-atentado-em-halle-%C3%A9-condenado-%C3%A0-pris%C3%A3o-perp%C3%A9tua/a-56010235

BRASIL, O Globo. "Autor de atentado antissemita na Alemanha em 2019 condenado à prisão perpétua." O Globo, 21 de janeiro de 2020. Disponível em: https://oglobo.globo.com/mundo/autor-de-atentado-antissemita-na-alemanha-em-2019-condenado-prisao-perpetua-24806297#:~:text=BERLIM%20%E2%80%94%20O%20autor%20do%20atentado,Kippur%2C%20na%20cidade%20de%20Halle

# Análise do compartilhamento de dados e proteção de privacidade no STF

Régis Martins
Samara Meneses Brito

## Introdução

O Supremo Tribunal Federal (STF) tem analisado diversas questões relacionadas à possibilidade ou não do compartilhamento de dados entre órgãos públicos e entre órgãos privados e públicos, especialmente em relação à proteção da privacidade e à segurança das informações. O debate gira em torno da compatibilidade desse compartilhamento com princípios constitucionais, como o direito à intimidade e à proteção de dados pessoais.

O STF tem enfatizado a necessidade de um equilíbrio entre a transparência e a proteção de dados, considerando aspectos como a finalidade do uso das informações, o consentimento dos titulares dos dados e a legalidade do compartilhamento.

O mega vazamento de dados de 223 milhões de brasileiros revelado em janeiro de 2021 é considerado um dos maiores na história do país e impulsionou discussões sobre a necessidade de uma aplicação rigorosa da Lei Geral de Proteção de Dados (LGPD). Dados pessoais como CPF, informações financeiras, de benefícios sociais e até fotos foram expostos, gerando preocupações sobre fraudes e uso indevido de informações sensíveis.

Este episódio também trouxe à tona a vulnerabilidade dos sistemas de segurança no Brasil e a necessidade de maior controle sobre o compartilhamento de dados entre entidades públicas e privadas, tema atualmente em debate no STF.

A Corte tem analisado a aplicação da Lei Geral de Proteção de Dados (LGPD) e suas implicações em casos específicos. Essa análise

é crucial para assegurar que o compartilhamento de dados entre órgãos públicos e privados não comprometa os direitos fundamentais dos cidadãos, ao mesmo tempo em que possibilita uma gestão pública mais eficiente e integrada.

No recorte da pesquisa que aqui relatamos, identificamos três ações diretas de inconstitucionalidade (ADI) e uma arguição de descumprimento de preceito fundamental (ADPF) que trataram sobre o tema, as ADIs 6387, 6529, 6649 e a ADPF 695.

**ADI 6387**

A ADI 6387 é um marco importante na discussão sobre a proteção de dados pessoais no Brasil. A ação foi proposta pelo Conselho Federal da OAB com pedido de medida cautelar contra o texto legal da Medida Provisória 954/2020 tendo como argumento que o repasse dessas informações violaria os dispositivos da Constituição Federal que asseguram a dignidade da pessoa humana, a inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas e o sigilo dos dados; outras ADIs, contra o inteiro teor do texto legal, foram impetradas por partidos políticos entre eles PSDB, PSB, PSOL e PDC do B, todas foram julgadas conjuntamente com a ADI 6387. As questões foram levantadas com o argumento de que a MP apresentava vícios de inconstitucionalidade, tanto formal quanto material, devido à não observância dos requisitos constitucionais necessários para a sua edição. Além disso, houve a alegação de violação das normas constitucionais relacionadas à dignidade da pessoa humana, à inviolabilidade da intimidade, à honra, à vida privada e à imagem das pessoas, bem como ao sigilo de dados.

Contextualizando a Medida Provisória nº 95, além dos requisitos de relevância e urgência foi utilizada pelo executivo como justificativa, o suporte à produção estatística oficial durante a emergência de saúde pública de importância internacional decorrente do coronavírus (Covid-19), de que trata a Lei nº 13.979, de 6 de fevereiro de 2020, além de ser atendida uma solicitação do

próprio IBGE para manter a continuidade de pesquisas antes feitas em visitas domiciliares, as quais naquele momento estavam impedidas em razão da pandemia de Covid-19, o referido órgão se comprometeu com o sigilo dos dados recebidos. Tínhamos desta forma a autorização em pleno auge da crise pandêmica, do compartilhamento de dados (relações de nomes, números de telefone e endereços de seus consumidores, sejam pessoas físicas ou jurídicas) por empresas de telecomunicações prestadoras de Serviço Telefônico Fixo Comutado e de Serviço Móvel Pessoal com a Fundação Instituto Brasileiro de Geografia e Estatística.

A Ministra Rosa Weber, relatora das ADIs, após as manifestações das partes e dos interessados na causa, reiterou as razões apresentadas e concedeu medidas liminares requeridas, destacando preocupações cruciais sobre a proteção de dados pessoais em meio à edição da Medida Provisória (MP). Em seu voto ressaltou que as informações previstas na MP estão relacionadas às pessoas naturais, e integram o âmbito de proteção das cláusulas constitucionais que asseguram a liberdade individual, a privacidade e o livre desenvolvimento da personalidade e, portanto, são considerados dados sensíveis, cuja manipulação deve respeitar os direitos constitucionais de liberdade, privacidade e desenvolvimento da personalidade.

Para a Ministra ainda, a falta de clareza na MP em relação ao objetivo e à amplitude da coleta de dados, assim como a ausência de explicações sobre a necessidade de fornecimento e uso desses dados, fragiliza a justificativa para sua implementação. A Ministra enfatizou que, sem essa definição, não é possível avaliar a adequação e a necessidade das medidas propostas, o que compromete o devido processo legal.

Além disso, a MP não incluiu mecanismos adequados para proteger os dados pessoais contra acessos não autorizados, vazamentos ou usos indevidos. Isso foi uma falha significativa, pois desrespeitou as exigências constitucionais de proteção de direitos fundamentais; para a Ministra igualmente não esclareceu a necessidade de fornecimento dos dados tampouco como seriam

efetivamente utilizados. Embora a crise sanitária demandasse políticas públicas fundamentadas em dados, a defesa dessas medidas não poderia justificar a violação de garantias constitucionais.

Segundo a relatora, o texto da Medida Provisória além de não delimitar o objeto da estatística a ser produzida, a finalidade específica e a sua amplitude, não deixou claro que a estatística a ser produzida está realmente relacionada à pandemia, que foi citada como justificativa. Essa falta de conexão explícita comprometeu a validade da MP, pois não se poderia discernir se a coleta de dados é realmente necessária para enfrentar a crise sanitária. Essa ambiguidade enfraqueceu a legitimidade da norma e levantou questões sobre a eficácia e a pertinência das informações que se pretendia coletar.

Rosa Weber aduziu ainda que a Medida Provisória falhou em fornecer mecanismos adequados para a proteção de dados pessoais, o que é essencial para evitar acessos não autorizados, vazamentos e usos indevidos. Essa ausência compromete o cumprimento das exigências constitucionais sobre a proteção de direitos fundamentais. A Ministra ressaltou que, mesmo diante da urgência provocada pela crise sanitária, a proteção dos direitos constitucionais, como a privacidade e a liberdade individual, deveria ser preservada. A necessidade de dados para a formulação de políticas públicas não pode servir como justificativa para desrespeitar garantias fundamentais. Ainda de acordo com a Ministra, é essencial que qualquer medida adotada respeite os limites estabelecidos pela Constituição, assegurando que as ações governamentais não comprometam direitos essenciais dos cidadãos.

O plenário do STF, decidiu suspender a aplicabilidade da Medida Provisória, bloqueando o compartilhamento de dados pessoais entre as empresas de telefonia e o IBGE. Essa decisão destaca a importância da proteção de dados pessoais, reconhecendo-os como informações que merecem tutela constitucional.

O julgamento reafirma que os dados pessoais não são apenas neutros, mas sim essenciais para a privacidade e dignidade dos indivíduos. Qualquer informação que possa identificar uma pessoa é, portanto, protegida pela Constituição, solidificando a ideia de que a coleta e o tratamento de dados devem ocorrer dentro de limites que respeitem os direitos fundamentais. Essa proteção é fundamental, especialmente em contextos em que o uso de dados pode impactar a liberdade e a privacidade dos cidadãos.

Quadro sinótico ADI 6387

| |
|---|
| **1 - Qual o pedido feito na ação? Ou seja, quais foram os elementos fáticos e legais? Quem propôs a ação?**<br>O pedido feito na ação versa sobre a constitucionalidade da MP 954/2020. As questões foram levantadas com o argumento de que a MP apresentava vícios de inconstitucionalidade, tanto formal quanto material, devido à não observância dos requisitos constitucionais necessários para a sua edição. Além disso, houve a alegação de violação das normas constitucionais relacionadas à dignidade da pessoa humana, à inviolabilidade da intimidade, à honra, à vida privada e à imagem das pessoas, bem como ao sigilo de dados. A ação foi proposta pelo Conselho Federal da OAB com pedido de medida cautelar, participou como *Amicus curiae* a Associação Data Privacy Brasil de Pesquisa; Laboratório de Políticas Públicas e Internet Lapin; IBGE. |
| **2 - Qual a efetiva decisão da Corte? A Corte (STF/TCF) privilegia a liberdade de expressão ou os direitos da personalidade?**<br>O Supremo Tribunal Federal reconheceu como direito fundamental autônomo a proteção dos dados pessoais. Decisão foi proferida pelo Pleno após ser referendada em decisão liminar da Ministra Rosa Weber. |
| **3 - As Cortes utilizam o princípio ou critério da proporcionalidade como método de solução dos conflitos entre a liberdade de expressão e os direitos de personalidade na rede?**<br>Foi utilizado por parte do Tribunal dos princípios da proporcionalidade e da razoabilidade |

Fonte: Quadro elaborado pelos autores

**ADI 6529**

A ADI 6529 foi também importante discussão sobre a proteção de dados pessoais no Brasil. A ação foi proposta pelos partidos políticos Rede Sustentabilidade e Partido Socialista Brasileiro, contra o decreto presidencial 10.445/2020, que condicionava o fornecimento de dados e conhecimentos à Agência Brasileira de Inteligência (Abin), refletindo preocupações sobre a centralização de informações sensíveis e a proteção de dados institucionais.

De acordo com os autores, a Abin tem poder de requisitar dados de investigações sigilosas, sigilo fiscal, relatórios do Conselho de Controle de Atividades Financeiras (Coaf) e dados de sigilo telefônico, "dentre tantas outras informações absolutamente sensíveis e sigilosas". O objeto de questionamento da ADI é o parágrafo único do artigo 4º da Lei 9.883/1999, que, segundo argumentam, possibilita o desvirtuamento de finalidade da Agência, uma vez que o poder requisitório de informações e dados de todos os integrantes do Sistema Brasileiro de Inteligência (Sisbin) depende de regulamentação pelo Presidente da República.

Os partidos políticos, ao traçarem um histórico dos decretos regulamentadores da Lei 9.883/1999 desde 2000, ressaltaram que a edição do Decreto 10.445/2020 aumentou a sensibilidade em torno da requisição de informações pela Agência Brasileira de Inteligência (Abin). Com a nova estrutura regimental, as hipóteses de requisição foram ampliadas, permitindo que o diretor-geral da Abin tenha acesso a informações sigilosas com uma simples solicitação.

Para os partidos, essa mudança não visava aprimorar o serviço de inteligência, mas sim facilitar o acesso a dados para investigações que podem ser direcionadas contra adversários políticos. Eles argumentaram que o decreto representaria mais um abuso do governo federal, visando facilitar investigações contra adversários políticos do presidente Jair Bolsonaro (2019-2022), permitindo o uso de dados para investigá-los. Essa crítica enfatizou as preocupações sobre a instrumentalização de informações sensíveis para fins políticos e solicitaram ao STF que estabelecesse

diretrizes claras para o compartilhamento de dados no Sistema Brasileiro de Inteligência (Sisbin).

A percepção de uso indevido de dados é central na crítica ao decreto, podendo infringir princípios constitucionais, como a transparência e o controle social sobre a atuação do governo e que seria necessária apenas uma requisição do presidente para que o diretor-geral da Abin obtivesse o conhecimento de informações sigilosas.

Os partidos buscaram então garantir que esse compartilhamento respeitasse os direitos fundamentais dos cidadãos, exigindo motivação adequada para as solicitações, razoabilidade nas demandas e proteção dos sigilos, que deveriam ser respeitados de acordo com a reserva de jurisdição. Essa discussão é crucial para preservar a democracia e evitar abusos no uso de informações sensíveis.

A decisão do STF, estabeleceu que o compartilhamento de informações pessoais nas atividades de inteligência deve seguir a legislação específica e priorizar o interesse público, foi um importante reforço à proteção dos direitos fundamentais. O Tribunal enfatizou a necessidade de equilibrar a segurança nacional com a transparência e a proteção da privacidade, garantindo que ações do governo sejam realizadas dentro dos limites constitucionais. Esse entendimento é crucial para assegurar a proteção dos direitos individuais e a transparência das ações do governo.

O Tribunal decidiu também que, o compartilhamento de informações pessoais nas atividades de inteligência deveria, entre outros pressupostos, observar legislação específica e sobretudo atender ao interesse público.

Ainda, de acordo com o julgado, há a possibilidade do agente público ser responsabilizado civilmente caso utilize os dados de forma contrária ao estabelecido pela legislação.

Segundo a Corte, o Estado ainda, poderá em ação regressiva acionar os servidores ou agentes políticos-públicos responsáveis por atos ilícitos que porventura vierem a ocorrer, visando desta forma o ressarcimento de eventuais danos ao erário público. Acaso

esta utilização de dados pelos agentes ocorra de maneira intencional esta responsabilização ocorrerá por improbidade administrativa com sanções disciplinares já previstas pela legislação em vigor.

Os desdobramentos refletem um debate mais amplo sobre a segurança e a liberdade, e como as instituições devem operar em um estado democrático, especialmente em tempos de polarização política.

Esse caso ilustra a tensão entre segurança e direitos civis, sublinhando a importância de salvaguardas institucionais em um contexto democrático, especialmente em períodos de forte polarização política.

Quadro sinótico ADI 6529

**1 - Qual o pedido feito na ação? Ou seja, quais foram os elementos fáticos e legais? Quem propôs a ação?**

A ação foi proposta pelos partidos políticos Rede Sustentabilidade e Partido Socialista Brasileiro, contra o decreto presidencial 10.445/2020, participou como *Amicus curiae* Associação dos Servidores da Agência Brasileira de Inteligência e Associação Nacional dos Oficiais de Inteligência. O decreto condicionava o fornecimento de dados e conhecimentos à Agência Brasileira de Inteligência (Abin), refletindo preocupações sobre a centralização de informações sensíveis e a proteção de dados institucionais. De acordo com os autores, a Abin teria poder de requisitar dados de investigações sigilosas, sigilo fiscal, relatórios do Conselho de Controle de Atividades Financeiras (Coaf) e dados de sigilo telefônico, "dentre tantas outras informações absolutamente sensíveis e sigilosas". O objeto de questionamento da ADI é o parágrafo único do artigo 4º da Lei 9.883/1999, que, segundo argumentam, possibilita o desvirtuamento de finalidade da Agência, uma vez que o poder requisitório de informações e dados de todos os integrantes do Sistema Brasileiro de Inteligência (Sisbin) depende de regulamentação pelo Presidente da República.

| |
|---|
| **2 - Qual a efetiva decisão da Corte? A Corte (STF/TCF) privilegia a liberdade de expressão ou os direitos da personalidade?**<br>O Tribunal decidiu que o compartilhamento de informações pessoais nas atividades de inteligência deve, entre outros pressupostos, respeitar a legislação específica e, sobretudo, atender ao interesse público. Além disso, conforme o julgamento, órgãos públicos que utilizarem os dados de maneira contrária aos parâmetros estabelecidos poderão ser responsabilizados civilmente. A Corte também afirmou que o Estado poderá, em ação regressiva, acionar os servidores ou agentes políticos responsáveis por atos ilícitos que eventualmente ocorram, visando o ressarcimento de danos ao erário público. Caso essa utilização de dados por parte dos agentes seja intencional, a responsabilização ocorrerá por improbidade administrativa, com sanções disciplinares já previstas na legislação vigente. |
| **3 - As Cortes utilizam o princípio ou critério da proporcionalidade como método de solução dos conflitos entre a liberdade de expressão e os direitos de personalidade na rede?**<br>Na ADI 6529, o STF utilizou o princípio da proporcionalidade como um critério fundamental para resolver os conflitos entre a liberdade de expressão e os direitos de personalidade. Esse princípio permite avaliar se a restrição à liberdade de expressão é necessária e adequada para proteger os direitos individuais, considerando, assim, o contexto específico da situação. O Tribunal analisou a importância da liberdade de expressão em uma sociedade democrática, mas também reconheceu que essa liberdade não é absoluta e pode ser limitada para garantir a proteção da dignidade e da privacidade das pessoas. O uso da proporcionalidade nesse caso buscou equilibrar esses interesses, garantindo que nenhuma das partes fosse desproporcionalmente prejudicada. |

Fonte: Quadro elaborado pelos autores

## A ADI 6649 - ADPF 695

A ADI 6649, proposta pelo Conselho Federal da Ordem dos Advogados do Brasil, e a ADPF 695, do Partido Socialista Brasileiro, foram agrupadas para julgamento no STF devido aos seus objetivos

semelhantes. Ambas contestavam o Decreto 10.046/2019, que regulamentava o compartilhamento de dados na administração pública federal e estabelecia o Cadastro Base do Cidadão.

As ações foram movidas com a alegação de que o Decreto 10.046/2019, do então presidente Jair Bolsonaro (2019-2022), que regulamenta a governança do compartilhamento de dados na administração pública federal e estabelecia o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados, configurava uma forma de vigilância excessiva sobre os cidadãos. Os autores sustentavam que isso simbolizava um controle exacerbado e inconstitucional por parte do Estado, violando direitos fundamentais e a privacidade dos indivíduos, ao promover uma vigilância excessiva sobre os cidadãos e um controle estatal inconstitucional.

Essa preocupação refletia um receio mais amplo sobre a utilização inadequada de dados pessoais, levantando questões sobre a transparência e a *accountability* no uso de informações sensíveis pelo governo. A decisão do STF, ao avaliar essas ações, buscou equilibrar a necessidade de compartilhar dados para fins administrativos com a proteção dos direitos dos cidadãos, reforçando a importância de limites claros e a observância da legislação pertinente, como a LGPD.

O STF, em decisão majoritária, reconheceu a legitimidade do compartilhamento de dados pessoais entre órgãos da administração pública, desde que respeitados critérios específicos. O relator, Ministro Gilmar Mendes, destacou que essa prática deve ser indispensável ao interesse público e limitada ao mínimo necessário para atender sua finalidade. Ele enfatizou a necessidade de alinhar esses critérios à Lei Geral de Proteção de Dados (LGPD), garantindo que a proteção de dados pessoais seja sempre respeitada.

O Tribunal determinou que o Comitê Central de Governança de Dados deve estabelecer critérios compatíveis com a LGPD e criar um sistema de registro de acessos para evitar abusos. Além disso, o uso inadequado de dados pode resultar em responsabilização civil para o órgão público, e os servidores ou agentes responsáveis

podem ser acionados em ação regressiva, especialmente em casos de má-fé, configurando improbidade administrativa.

Em seu voto, o Ministro relator Gilmar Mendes afirmou que o compartilhamento de dados é possível, desde que respeitados determinados parâmetros. Ele enfatizou que essa permissão deve ser considerada legítima, mas com limites claros: as informações compartilhadas devem ser indispensáveis ao interesse público e restringidas ao mínimo necessário para cumprir sua finalidade.

O Ministro também destacou que os requisitos para esse compartilhamento devem seguir integralmente as garantias e preceitos da Lei Geral de Proteção de Dados (LGPD – Lei 13.709/2018), adaptados ao contexto do setor público. Essa abordagem visa garantir que a proteção dos dados pessoais dos cidadãos seja respeitada, promovendo um equilíbrio entre a eficiência administrativa e os direitos individuais. Além disso, o Tribunal determinou que o Comitê deve implementar um sistema de registro de acessos, o que visa prevenir abusos no uso de informações. Essa abordagem reforça a importância da transparência e da responsabilização na gestão de dados, assegurando que o compartilhamento ocorra de maneira controlada e justificada, em conformidade com as garantias legais estabelecidas, desta forma o reconhecimento da necessidade de limites claros é crucial para evitar abusos e assegurar a transparência nas ações do governo.

O Tribunal determinou ainda que o Comitê deve implementar um sistema de registro de acessos, o que visa prevenir abusos no uso de informações.

A decisão do STF, reiterando os princípios da ADI 6529, estabelece que órgãos públicos que utilizarem dados de forma contrária aos parâmetros definidos poderão ser responsabilizados civilmente. Além disso, o Estado poderá acionar, em ação regressiva, os servidores ou agentes políticos responsáveis por eventuais atos ilícitos, buscando o ressarcimento de danos ao erário público.

Caso a utilização inadequada de dados ocorra de forma intencional, os responsáveis poderão enfrentar responsabilização

por improbidade administrativa, o que inclui sanções disciplinares conforme a legislação vigente. Essa estrutura de responsabilização é fundamental para garantir a integridade e a transparência na gestão de dados, protegendo os direitos dos cidadãos e assegurando que o uso de informações pessoais seja feito de maneira ética e legal.

Quadro sinótico ADI 6649 e ADPF 695

| |
|---|
| **1 - Qual o pedido feito na ação? Ou seja, quais foram os elementos fáticos e legais? Quem propôs a ação?**<br>A ADI 6649, proposta pelo Conselho Federal da Ordem dos Advogados do Brasil, e a ADPF 695, do Partido Socialista Brasileiro, foram agrupadas para julgamento no STF devido aos seus objetivos semelhantes. Ambas contestavam o Decreto 10.046/2019, que regulamentava o compartilhamento de dados na administração pública federal e estabelecia o Cadastro Base do Cidadão. As ações foram movidas com a alegação de que o Decreto 10.046/2019, do então presidente Jair Bolsonaro, que regulamenta a governança do compartilhamento de dados na administração pública federal e estabelecia o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados, configurava uma forma de vigilância excessiva sobre os cidadãos. Participou como *Amicus curiae* Associação dos servidores da ABIN; Associação Data Privacy Brasil de Pesquisa; Associação Lawgorithm de Pesquisa em Inteligência Artificial; Instituto Beta para Democracia e Internet; Laboratório de Políticas Públicas e Internet Lapin; IBIDEM; Intervozes; Coletivo Brasil de Comunicação Social; Instituto Mais Cidadania. |
| **2 - Qual a efetiva decisão da Corte? A Corte (STF/TCF) privilegia a liberdade de expressão ou os direitos da personalidade?**<br>Em sessão plenária, decidiu o Supremo Tribunal Federal (STF), por maioria dos votos, que os órgãos e as entidades da administração pública federal (direta e indireta) poderão compartilhar dados pessoais entre si, mas sempre com a observância em alguns critérios. |

| |
|---|
| **3 - As Cortes utilizam o princípio ou critério da proporcionalidade como método de solução dos conflitos entre a liberdade de expressão e os direitos de personalidade na rede?**<br>Na ADI 6649 e na ADPF 695, o STF também aplicou o princípio da proporcionalidade como um método para resolver os conflitos entre a liberdade de expressão e os direitos de personalidade. O Tribunal examinou a necessidade de equilibrar esses direitos, reconhecendo que, embora a liberdade de expressão seja essencial em uma sociedade democrática, ela pode ser limitada para proteger a dignidade e a privacidade dos indivíduos. Nesse contexto, a proporcionalidade foi utilizada para avaliar se as restrições impostas à liberdade de expressão eram adequadas, necessárias e proporcionais em relação aos direitos de personalidade que estavam em jogo. Essa abordagem busca garantir que nem a liberdade de expressão nem os direitos de personalidade sejam desrespeitados de forma excessiva. |

Fonte: Quadro sinótico elaborado pelos autores.

## Considerações

A análise desses quatro casos demonstra que o compartilhamento de dados pessoais é viável, contanto que sejam respeitados os parâmetros estabelecidos pela legislação, especialmente a Lei Geral de Proteção de Dados (LGPD), e as diretrizes reafirmadas pelo STF. Essas decisões enfatizam a necessidade de justificação formal e prévia para o compartilhamento, limites de uso que atendam ao interesse público e a implementação de mecanismos de controle, como registros de acesso, para evitar abusos.

Assim, os casos analisados reafirmam que o compartilhamento de dados pessoais é viável, desde que respeitados os limites e parâmetros estabelecidos pela legislação, garantindo a proteção dos direitos dos cidadãos. Essa abordagem equilibra a necessidade de eficiência na administração pública com a proteção da privacidade e dos direitos individuais.

Dessa forma, o equilíbrio entre a eficiência administrativa e a proteção dos direitos individuais é crucial, assegurando que o uso de dados pessoais ocorra de maneira responsável e transparente. Essa abordagem busca promover um ambiente onde a segurança e a privacidade dos cidadãos sejam devidamente respeitadas.

## Referências


BRASIL, G1. Vazamento de dados de 223 milhões de brasileiros: o que se sabe e o que falta saber. 28 jan. 2021. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/2021/01/28/vazamento-de-dados-de-223-milhoes-de-brasileiros-o-que-se-sabe-e-o-que-falta-saber.ghtml

BRASIL. **Supremo Tribunal Federal**. AÇÃO DIRETA DE INCONSTITUCIONALIDADE 6.529. Requerente: Rede Sustentabilidade. Relatora: Min. Cármem Lúcia, 11 de outubro de 2021. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=757870910. Acesso em: set./2024.

BRASIL. **Supremo Tribunal Federal**. Ação Direta de Inconstitucionalidade 6.649. Requerente: Conselho Federal da Ordem dos Advogados do Brasil. Relator: Min. Gilmar Mendes, 15 de setembro de 2022. Disponível em: https://images.jota.info/wp-content/uploads/2022/09/voto-adi-6649-e-adpf-695-1.pdf. Acesso em: out./2024.

BRASIL. **Supremo Tribunal Federal**. Arguição de Descumprimento de Preceito Fundamental 695. Requerente: Partido Socialista Brasileiro. Relator: Min. Gilmar Mendes, 15 de setembro de 2022. Disponível em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=5938693. Acesso em: out./2024.

BRASIL. **Supremo Tribunal Federal**. Medida Cautelar na Ação Direta de Inconstitucionalidade 6837. Medida Provisória 954/2020. Requerente: Conselho Federal da Ordem dos Advogados do Brasil. Relatora: Min. Rosa Weber, 24 de abril de 2020. Disponível em: http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADI6387MC.pdf. Acesso em: set./2024.

# EIXO INVESTIGAÇÃO CRIMINAL

# O sigilo de dados e a garantia da privacidade nas investigações criminais

Carlo José Napolitano
Deborah Cunha Teodoro
Isadora Pinto de Sousa
Tatiana Stroppa
Lucas Catib Laurentiis

Nas atuais sociedades da informação, as múltiplas atividades comunicativas, profissionais, pessoais e interpessoais vêm sendo praticadas cada vez mais por meio de modernos aparelhos celulares (*smartphones*) com alta capacidade de memória que possibilitam um enorme armazenamento de dados relacionados aos seus titulares e de terceiros que com ele tenham interagido de alguma forma (Rebellato, 2021).

Segundo o autor (2021), a criminalidade também está usufruindo destes recursos tecnológicos para praticar crimes, exigindo a adoção de novos mecanismos de investigação criminal, dentre os quais, o acesso ao conteúdo de dados armazenados em aparelhos celulares, visto que mecanismos de criptografia tornaram obsoletos os meios tradicionais de investigação disponíveis no ordenamento jurídico brasileiro. Por outro lado, não houve evolução legislativa condizente com esta realidade digital, demandando das cortes uma definição quanto à necessidade de autorização judicial para o acesso aos dados em distintas situações.

Nesse panorama, a facilitação comunicativa e o desenvolvimento exponencial de tecnologias de produção, captação, compartilhamento e armazenamento em massa de dados vêm impactando o exercício dos direitos de expressão, de privacidade, intimidade e proteção de dados e, consequentemente,

exigindo uma (re)discussão dos limites constitucionais relacionados à tutela de tais direitos no ambiente digital.

Justamente nesse complexo e intrincado cenário é que o presente capítulo apresenta e analisa dois processos, ainda em andamento no Supremo Tribunal Federal, que tratam da proteção de dados pessoais, direito à privacidade e ao sigilo das comunicações diante de investigações criminais. São os Recursos Extraordinários 1.301.250 e 1.042.075.

**Apresentação e análise do Recurso Extraordinário 1.301.250**

O Recurso Extraordinário 1.301.250 foi interposto pelas empresas Google Brasil Internet Ltda. e Google LLC, que questionaram a constitucionalidade da determinação da Justiça Carioca para que as empresas fornecessem a "identificação dos IP's ou "DEVICE IDs" que tenham se utilizado do Google Busca (seja através do aplicativo de celular ou sua versão WEB), no período compreendido entre o dia 10/03/2018 a 14/03/2018, para realizar consultas dos seguintes parâmetros de pesquisa: "Mariele Franco"; "Vereadora Mariele"; "Agenda Vereadora Mariele"; "Casa das Pretas"; "Rua dos Inválidos, 122" ou "Rua Dos Invalidos".

O caso de fundo tratava da investigação acerca dos homicídios da vereadora Mariele Franco[7] e de seu motorista Anderson Gomes no dia 14 de março de 2018 na região central do Rio de Janeiro.

[7] Marielle Franco foi uma vereadora e defensora dos direitos humanos no Rio de Janeiro, assassinada em 14 de março de 2018, quando seu carro foi alvejado por tiros enquanto ela retornava de um evento no centro da cidade. O ataque resultou na morte de Marielle e de seu motorista, Anderson Gomes. Marielle era uma mulher negra e ativista, conhecida por sua luta contra a violência policial e por defender os direitos das minorias, incluindo a população negra e LGBTQIA+. Seu assassinato gerou uma onda de protestos e indignação no Brasil e no mundo, levantando questões sobre a segurança pública, a violência política e a impunidade em casos de assassinatos de figuras públicas. As investigações iniciais enfrentaram diversos obstáculos, incluindo a resistência das autoridades e a falta de transparência. Relato elaborado por Isadora Pinto de Souza.

O Recurso Extraordinário foi protocolado no Supremo Tribunal Federal, em 26 de novembro de 2020, nos autos de um Mandado de Segurança, no qual foi negado, pelo Tribunal de Justiça do Rio de Janeiro e pelo Superior Tribunal de Justiça, o pedido que questionava a decisão do Juiz da 4ª Vara Criminal da Cidade do Rio de Janeiro, a qual determinou o fornecimento da identificação dos IPs, conforme mencionado.

No Recurso Extraordinário, as empresas alegaram violações dos artigos 5º, incisos X (*são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação*) e XII (*é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal*), e 93, inciso IX (*todos os julgamentos dos órgãos do Poder Judiciário serão públicos, e fundamentadas todas as decisões, sob pena de nulidade, podendo a lei limitar a presença, em determinados atos, às próprias partes e a seus advogados, ou somente a estes, em casos nos quais a preservação do direito à intimidade do interessado no sigilo não prejudique o interesse público à informação*) da Constituição Federal de 1988, além de sustentarem que a determinação era desproporcional, por ser a medida inadequada, desnecessária e desproporcional.

Em 24 de abril de 2023, foram admitidos no RE, na qualidade de *amici curiae*, o projeto do movimento negro Educação e Cidadania de Afrodescendentes e Carentes (EDUCAFRO), o Instituto Brasileiro de Ciências Criminais (IBCCRIM) e o Instituto de Tecnologia e Sociedade do Rio de Janeiro (ITS Rio) por preencherem os requisitos legais, além de demonstrarem utilidade e conveniência da atuação, considerado o contexto argumentativo do feito, a relevância da participação, bem como a amplitude e adequação da representatividade. Em contrapartida, foi indeferido o pedido do "Facebook, Inc.", em razão da inaptidão contributiva específica e da carência de representatividade adequada. Posteriormente, em 15 de setembro de 2023, foi admitido, na

condição de *amicus curiae*, o Ministério Público do Estado de Minas Gerais (MPMG), mas negados os pedidos do Ministério Público do Estado de Rondônia (MPRO), em 25 de setembro de 2023, e, em 28 de setembro de 2023, o do Instituto de Defesa do Direito de Defesa Márcio Thomaz Bastos e o da Associação Internetlab de Pesquisa em Direito e Tecnologia.

Em 02 de outubro de 2023, a Ministra Rosa Weber (Relatora) deu provimento ao Recurso Extraordinário para conceder a ordem mandamental e, em consequência, cassar o item referente ao fornecimento dos IPs, determinado em 27.8.2018, pelo Juízo de primeiro grau, facultando que outra decisão fosse proferida, desde que observados os limites formais e materiais dos direitos fundamentais à privacidade, à proteção de dados pessoais e ao devido processo legal, e propunha, no seu voto, a fixação da seguinte tese (Tema 1.148) de repercussão geral:

> À luz dos direitos fundamentais à privacidade, à proteção dos dados pessoais e ao devido processo legal, o art. 22 da Lei 12.965/2014 (Marco Civil da Internet) não ampara ordem judicial genérica e não individualizada de fornecimento dos registros de conexão e de acesso dos usuários que, em lapso temporal demarcado, tenham pesquisado vocábulos ou expressões específicas em provedores de aplicação. (BRASIL, RE 1.301.250).

Importa observar que ainda não há uma decisão definitiva da Corte. Contudo, com base no voto proferido pela Ministra Relatora, é possível concluir, provisoriamente, que a decisão privilegiou a aplicação do direito à privacidade e à proteção de dados em detrimento do direito à informação e à busca da verdade real, princípio esse que informa a investigação processual penal.

Por fim, em relação ao uso ou não do princípio da proporcionalidade, ainda é prematuro para dizer se o STF irá se pautar por esse critério; contudo, é possível inferir que a Corte terá que analisar essa questão, já que esse foi um dos argumentos das empresas Google ao ajuizar o Recurso Extraordinário no STF.

Nesse sentido, em seu voto a Ministra Relatora Rosa Weber assim se manifestou:

> (...) **desproporcionalidade** da medida adotada, o que pode se verificar da própria delimitação temporal estabelecida. Os delitos objeto de investigação foram cometidos, segunda a própria decisão do Juízo de primeiro grau, por volta das 21h do dia 14 de março de 2018. O pedido da autoridade policial, acolhido pelo Juízo competente, foi o de encaminhamento dos endereços de IP e dos Devices ID's de todos que pesquisaram, no Google Search, o nome da Vereadora Marielle Franco, inclusive, ainda que por curto lapso, após o seu homicídio. Natural, dada a repercussão na impressa nacional e internacional dos homicídios qualificados da Vereadora Marielle Franco e de Anderson Gomes, que pessoas dos mais diversos matizes político-ideológicos tenham realizado, após o delito, pesquisas a respeito da figura pública em questão. Ou seja, um número gigantesco de usuários não envolvidos em quaisquer atividades ilícitas, nos termos da decisão objurgada, teria seus sigilos afastados, a demonstrar indevida devassa e a sua absoluta **desproporcionalidade** em razão do excesso da medida. (BRASIL, RE 1.301.250).

Logo, é possível deduzir que o plenário do STF terá que analisar a proporcionalidade quando do julgamento definitivo pela corte.

Quadro sinóptico do RE 1.301.250

| |
|---|
| **1 - Qual o pedido feito na ação? Ou seja, quais foram os elementos fáticos e legais? Quem propôs a ação?** |
| Trata-se de Recurso Extraordinário interposto pelas empresas Google Brasil Internet Ltda. e Google LLC, nos autos de um Mandado de Segurança, no qual foi negado, pelo Tribunal de Justiça do Rio de Janeiro e pelo Superior Tribunal de Justiça, o pedido que questionava a decisão do Juiz da 4ª Vara Criminal da Cidade do Rio de Janeiro, que havia determinado o fornecimento da "identificação dos IP's ou "DEVICE IDs" que tenham se utilizado do Google Busca (seja através do aplicativo de celular ou sua versão WEB), no período compreendido |

entre o dia 10/03/2018 a 14/03/2018, para realizar consultas dos seguintes parâmetros de pesquisa: "Mariele Franco"; "Vereadora Mariele"; "Agenda Vereadora Mariele"; "Casa das Pretas"; "Rua dos Inválidos, 122" ou "Rua Dos Invalidos", devido à investigação dos homicídios da vereadora Mariele Franco e de seu motorista Anderson Gomes no dia 14 de março de 2018 na região central do Rio de Janeiro. As empresas alegaram violações dos artigos 5º, incisos X (*são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação*) e XII (*é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal*), e 93, inciso IX (*todos os julgamentos dos órgãos do Poder Judiciário serão públicos, e fundamentadas todas as decisões, sob pena de nulidade, podendo a lei limitar a presença, em determinados atos, às próprias partes e a seus advogados, ou somente a estes, em casos nos quais a preservação do direito à intimidade do interessado no sigilo não prejudique o interesse público à informação*) da Constituição Federal, além de sustentarem que a determinação era desproporcional, inadequada e desnecessária.

**2 - Qual a efetiva decisão da Corte? A Corte (STF/TCF) privilegia a liberdade de expressão ou os direitos da personalidade?**

Embora o RE ainda esteja pendente de julgamento, o voto proferido pela Ministra Relatora Rosa Weber privilegiou o direito à privacidade e à proteção de dados em detrimento do direito à informação e à busca da verdade real, princípio esse que informa a investigação processual penal.

**3- As Cortes utilizam o princípio ou critério da proporcionalidade como método de solução dos conflitos entre a liberdade de expressão e os direitos de personalidade na rede?**

Por enquanto, o voto da relatora do RE mencionou a "**desproporcionalidade** da medida adotada", uma vez que a repercussão na impressa nacional e internacional dos homicídios qualificados da vereadora Marielle Franco e de seu motorista Anderson Gomes levaria um grande número de usuários não envolvidos em quaisquer atividades ilícitas a terem seus sigilos afastados, numa

indevida devassa e absoluta "**desproporcionalidade** da medida adotada". Logo, é possível deduzir que, quando houver o julgamento definitivo pela corte, o plenário do Supremo Tribunal Federal deverá levar em consideração o critério da proporcionalidade entre os direitos fundamentais em conflito para proferir sua decisão, até porque esse foi um dos argumentos das empresas Google que ajuizaram o Recurso Extraordinário no STF.

Fonte: Quadro elaborado pelos autores

## Apresentação e análise do Recurso Extraordinário com Agravo 1.042.075

O Recurso Extraordinário com Agravo (ARE) 1.042.075 foi interposto pelo Ministério Público do Estado do Rio de Janeiro em 21 de abril de 2017. O processo teve como elemento fático o caso de uma pessoa investigada, processada e condenada por um crime de roubo ocorrido na cidade do Rio de Janeiro[8].

[8] O Ministério Público do Estado do Rio de Janeiro ofereceu denúncia contra Guilherme Carvalho Farias, por roubo qualificado com uso de violência e grave ameaça. O réu, junto a um comparsa não identificado, abordou a vítima, Aparecida Caetano de Almeida, no dia 21 de maio de 2013, às 12h50min, na Rua Alfredo Pinto, esquina com a Rua Conde de Bonfim, próxima ao Banco Citibank, no bairro Tijuca, Rio de Janeiro. A vítima saía da agência bancária quando foi surpreendida por Guilherme, que, portando uma arma de fogo e agindo em comunhão com seu comparsa, anunciou o assalto. A vítima tentou resistir, segurando sua bolsa, mas foi empurrada pelo denunciado, caindo ao chão. Mesmo com a vítima caída, o réu continuou as agressões, batendo a cabeça dela contra o chão, e em seguida conseguiu subtrair a bolsa. Dentro da bolsa havia dois celulares (Apple e Sony Ericsson), diversos documentos, cartões bancários, folhas de cheque e a quantia de R$ 5.550,00 em espécie. Após o assalto, o réu fugiu em uma motocicleta que estava sendo conduzida por seu comparsa. Durante a fuga, Guilherme deixou cair um celular, que foi recolhido por policiais civis. Na perícia, o aparelho continha fotografias que permitiram a identificação do acusado. No dia seguinte, após diligências realizadas pela polícia, Guilherme foi preso e reconhecido prontamente pela vítima na delegacia como o autor do roubo. Os policiais civis envolvidos na identificação e prisão foram Amaury Dias Junior, Mayke da Silva Oliveira e Marcelo Santos Marques Rezende. Relato fático desenvolvido pela co-autora Isadora Pinto de Sousa.

A polícia somente chegou a essa pessoa, porque, após a execução do crime, esse suposto criminoso, durante a fuga, deixou cair um aparelho celular, o qual foi apreendido por policiais civis que, por sua vez, verificaram a existência de fotografias do implicado na memória do aparelho, o que norteou a realização de diligências que possibilitaram a identificação e prisão do assaltante.

O réu foi condenado em primeira instância, recorrendo ao Tribunal de Justiça do Rio de Janeiro que o absolveu. Em sua decisão, o TJRJ entendeu que houve "flagrante e indisfarçável quebra da proteção constitucional incidente sobre a inviolabilidade do sigilo dos dados e das comunicações telefônicas ali existentes, o que apenas poderia se dar, por exceção, mediante expressa autorização judicial".

O MPRJ ajuizou então o mencionado RE, questionando a decisão do TJRJ. No recurso, o MPRJ alega, em síntese, que não houve ofensa ao princípio constitucional da inviolabilidade do sigilo das comunicações telefônicas e que é possível o acesso a registros e informações contidos em aparelho de telefone celular apreendido como instrumento ou objeto de conduta delitiva sem o respectivo mandado judicial.

Ao discutir a licitude da prova produzida durante o inquérito policial referente ao acesso, sem autorização judicial, de registros e informações contidas em aparelho de telefonia celular relacionado à conduta delitiva, hábeis a identificar o agente do crime, passa-se à análise do artigo 5º, incisos XII e LVI, da CRFB/1988:

> XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal;
> LVI - são inadmissíveis, no processo, as provas obtidas por meios ilícitos. (CRFB/1988).

Para o Ministro Dias Toffoli, relator do caso, a matéria tratada no ARE 1042075 tem natureza constitucional, pois diz respeito à inviolabilidade do sigilo das comunicações telefônicas (artigo 5°, inciso XII, da CF/1988) e à impossibilidade de utilização, no processo, de provas supostamente obtidas por meio ilícito:

> Essas garantias constitucionais mantêm estreito vínculo entre si e regulam e limitam a obtenção, a produção e a valoração das provas destinadas ao Estado, o que, no caso, será decisivo para se determinar a legitimidade da atuação da autoridade policial no papel de proceder à coleta de elementos e informações hábeis a viabilizar a persecução penal. (MPRJ, 2017).

O tema, segundo o relator, extrapola o interesse subjetivo das partes, dada sua relevância, além de ser uma oportunidade para se consolidar a orientação do STF a esse respeito: "o julgamento do tema, sob a égide da repercussão geral, possibilitará a fruição de todos os benefícios daí decorrentes" (MPRJ, 2017).

Em 31 de outubro de 2017, Toffoli reconheceu a existência de repercussão geral da matéria, tendo o Plenário Virtual do STF referendado a decisão, por unanimidade, em 24 de novembro do mesmo ano, reputando constitucional a questão suscitada.

Em 16 de novembro de 2018, o relator do caso indeferiu os pedidos apresentados pelos Instituto Brasileiro de Ciências Criminais (IBCCRIM), Instituto de Garantias Penais (IGP), ARTIGO 19 BRASIL e WITNESS, e em 03 de abril de 2019, da Defensoria Pública da União, para ingressar na ação na condição de *amici curiae*. Naquela oportunidade, a intervenção do IBCCRIM na causa foi impedida sob o argumento de ausência de representatividade e não demonstração da utilidade nas informações prestadas. Já o IGP, ARTIGO 19 BRASIL, WITNESS e a Defensoria Pública da União tiveram seus pedidos negados sob a justificativa de que, como o processo já havia sido liberado para a pauta de julgamento, não havia sido cumprido o requisito da oportunidade. Todavia, em 1° de dezembro de 2023, foram

deferidos os pedidos de ingresso do IBCCRIM e do Ministério Público do Estado de Santa Catarina (MP-SC) como "amigos da corte", entendendo que ambos atendiam os requisitos de relevância da matéria debatida e de representatividade dos postulantes.

O caso ainda está pendente de julgamento pela Corte. Contudo, neste caso, quatro ministros (o relator Dias Toffoli e os Ministros Gilmar Mendes, Edson Fachin e Flávio Dino) já proferiram os seus votos no sentido de não conferir provimento ao recurso. Tanto no voto do Ministro relator quanto no do Ministro que apresentou divergência (Gilmar Mendes), há propostas de fixação de teses para casos semelhantes.

Ambos votos vão no sentido de exigir ordem judicial para o acesso aos dados telefônicos e também há a menção do uso do critério da proporcionalidade para a solução do conflito com a justificativa, por parte do judiciário, da necessidade e adequação da medida: "O acesso a registro telefônico, agenda de contatos e demais dados contidos em aparelhos celulares apreendidos no local do crime atribuído ao acusado depende de prévia decisão judicial que justifique, com base em elementos concretos, a necessidade e a adequação da medida e delimite a sua abrangência à luz dos direitos fundamentais à intimidade, à privacidade e ao sigilo das comunicações e dados dos indivíduos (CF, art. 5º, X e XX)."

Verifica-se, portanto, que neste caso, mesmo que de forma provisória, o STF privilegiou a privacidade em detrimento do poder estatal de realizar a investigação policial.

Justamente nesse sentido, a massificação do uso de *smartphones* conectados na rede de computadores, com o imenso armazenamento de dados pessoais e de informações que podem ser acessados em investigações, demonstram a necessidade de repensar uma equação que fixe os parâmetros constitucionais que protegem os direitos fundamentais, por um lado, e, por outro, assegure a eficiência na atividade penal investigativa que deve ser promovida pelo Estado.

Quadro sinóptico do ARE 1.042.075

| |
|---|
| **1 - Qual o pedido feito na ação? Ou seja, quais foram os elementos fáticos e legais? Quem propôs a ação?**<br>Trata-se de Recurso Extraordinário com Agravo (ARE), interposto pelo Ministério Público do Estado do Rio de Janeiro (MPRJ), em que se discute a licitude da prova produzida durante o inquérito policial referente ao acesso, sem autorização judicial, de registros e informações contidas em aparelho de telefonia celular relacionado à conduta delitiva, hábeis a identificar o agente do crime. Em análise, o artigo 5º, incisos XII e LVI, da CRFB/1988. |
| **2 - Qual a efetiva decisão da Corte? A Corte (STF/TCF) privilegia a liberdade de expressão ou os direitos da personalidade?**<br>O caso ainda está pendente de julgamento pela Corte, todavia, quatro Ministros (o relator Dias Toffoli e os Ministros Gilmar Mendes, Edson Fachin e Flávio Dino) já proferiram votos no sentido de não conferir provimento ao recurso, o que privilegiaria os direitos da personalidade, como os direitos fundamentais à privacidade, intimidade, ao sigilo das comunicações e à proteção dos dados pessoais, inclusive nos meios digitais, conforme dispõe o artigo 5º, incisos X, XII e LXXIX, da CRFB/1988, em detrimento da liberdade de expressão que, neste ARE, decorreria da autorização para o poder estatal realizar a investigação policial independentemente de ordem judicial. |
| **3- As Cortes utilizam o princípio ou critério da proporcionalidade como método de solução dos conflitos entre a liberdade de expressão e os direitos de personalidade na rede?**<br>Os votos dos Ministros Gilmar Mendes e Edson Fachin, que negam provimento ao ARE, respaldando-se na exigência de ordem judicial para o acesso aos dados telefônicos, mencionam a utilização do critério da proporcionalidade para a solução do conflito sob a justificativa da necessidade e adequação da medida: "O acesso a registro telefônico, agenda de contatos e demais dados contidos em aparelhos celulares apreendidos no local do crime atribuído ao acusado depende de prévia decisão judicial que justifique, com base em elementos concretos, a necessidade e a adequação da medida e delimite a sua abrangência à luz dos direitos fundamentais à intimidade, à privacidade e ao sigilo das comunicações e dados dos indivíduos (CF, art. 5º, X e XX).". |

Fonte: Quadro elaborado pelos autores.

## Considerações sobre os julgamentos

Os dois recursos, o RE 1.301.250 e o ARE 1.042.075, são *leading cases* e determinarão orientações e interpretações futuras do STF em relação a julgamentos semelhantes.

Conclui-se, neste capítulo, que o "sigilo das comunicações é não só um corolário da garantia da livre expressão de pensamento; exprime também aspecto tradicional do direito à privacidade e à intimidade" (Mendes; Branco, 2013. p. 293).

Essas são as sínteses das decisões que poderão ser melhor detalhadas quando do julgamento final de aludidos recursos.

## Referências


Após recurso do MPRJ, STF discutirá acesso aos dados em celulares encontrados em locais de crime. **MPRJ - Ministério Público do Estado do Rio de Janeiro, Notícia, 29/11/2017**. Disponível em: https://mca.mp.rj.gov .br/web/guest/visualizar?noticiaId=51507. Acesso em: 8 de maio de 2024.

Brasil**. Supremo Tribunal Federal. RE 1.301.250**. Disponível em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=6059876. Acesso em: maio de 2024.

Brasil. **Supremo Tribunal Federal. RE 1.042.075**. Disponível em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=5173898. Acesso em: maio de 2024.

Mendes, G. F.; Branco, P. G. G. (2013). **Curso de Direito Constitucional**. São Paulo: Saraiva.

Rebellato, L. F. B. (2021). A análise constitucional do sigilo e da privacidade nas investigações criminais: o acesso a dados armazenados em aparelhos celulares. **Dissertação de Mestrado**. Faculdade de Direito, Universidade de São Paulo, SP. Disponível em: https://doi.org/10.1 1606/D.2.2021.tde-08072022-114811. Acesso em: maio de 2024.

# EIXO DIVULGAÇÃO DE PROCESSOS

# Limites do Direito à Informação diante das novas tecnologias: reflexões sobre a publicidade processual em ambientes digitais a partir do Tema 1141 do STF

Arthur Almeida de Oliveira
Renato Sobhie Zambonatto

A era digital trouxe inúmeros avanços na maneira como lidamos com informações, especialmente no que diz respeito à publicidade de dados processuais e ao acesso público a informações jurídicas. O Supremo Tribunal Federal (STF) está no centro de um debate que envolve a responsabilização por divulgação de informações processuais em sites na internet, especificamente em casos sem a proteção do segredo de justiça, e a possibilidade ou obrigação de remoção de tais conteúdos.

Este assunto, formalizado no Tema 1141 (Brasil, 2021) no RE 1307386, traz à tona questões cruciais sobre a relação entre a transparência processual e a privacidade individual, especialmente no contexto das ferramentas digitais, que acabam por tornar essas informações acessíveis a todos.

A publicidade dos atos processuais é um princípio fundamental garantido pela Constituição Federal. Ela tem como objetivo assegurar a transparência e o acesso público às informações do Poder Judiciário. A Resolução 121/2010 do Conselho Nacional de Justiça (CNJ), por exemplo, determina que processos judiciais, salvo aqueles que tramitam sob segredo de justiça, sejam acessíveis eletronicamente ao público em geral:

> A consulta aos dados básicos dos processos judiciais será disponibilizada na rede mundial de computadores (internet), assegurado o direito de acesso a informações processuais a toda e qualquer pessoa, independentemente de prévio cadastramento ou de demonstração de interesse (Brasil, 2010, Art. 1).

Essa medida busca garantir a publicidade processual como uma regra, fortalecendo o controle social e a confiança no sistema judiciário. Os artigos da Constituição Federal, particularmente o Art. 5º, que trata sobre os direitos fundamentais, asseguram o direito à informação (incisos XIV e XXXIII) e a liberdade de expressão (inciso IX), equilibrados pelo direito à privacidade e à inviolabilidade da intimidade (inciso X):

> IX - é livre a expressão da atividade intelectual, artística, científica e de comunicação, independentemente de censura ou licença; [...] XIV - é assegurado a todos o acesso à informação e resguardado o sigilo da fonte, quando necessário ao exercício profissional; [...] X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação (Brasil, 1988, Art. 5).

Outros dispositivos constitucionais, como os Art. 37, *caput*, e Art. 93, IX, reforçam que a administração pública e o Poder Judiciário devem operar de forma transparente, garantindo a publicidade dos atos processuais como um direito do cidadão.

> Art. 37. A administração pública direta e indireta de qualquer dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios obedecerá aos princípios de legalidade, impessoalidade, moralidade, publicidade e eficiência. [...] Art. 93. Lei complementar, de iniciativa do Supremo Tribunal Federal, disporá sobre o Estatuto da Magistratura, observados os seguintes princípios: IX todos os julgamentos dos órgãos do Poder Judiciário serão públicos, e fundamentadas todas as decisões, sob pena de nulidade, podendo a lei limitar a presença, em determinados atos, às próprias partes e a seus advogados, ou somente a estes, em casos nos quais a preservação do direito à intimidade do interessado no sigilo não prejudique o interesse público à informação (Brasil, 1988, Art. 37-93).

No entanto, mesmo que essa publicidade tenha o objetivo de garantir a clareza e a transparência, surgem questões sobre o impacto da divulgação de certos dados pessoais e processuais na

vida privada das partes envolvidas. No contexto digital atual, as informações processuais publicadas pelos órgãos oficiais podem ser facilmente replicadas em plataformas públicas e acessadas por qualquer pessoa, gerando potencial de exposição indevida e até desinformação.

O caso do Tema 1141 coloca essa questão em evidência, com implicações diretas sobre o equilíbrio entre a transparência do Judiciário e o direito à privacidade das partes envolvidas. Plataformas como Google e Escavador têm sido alvo de ações que buscam proteger as partes de possíveis danos causados pela exposição indevida dessas informações, mesmo quando elas são publicamente acessíveis de acordo com a lei.

Ao mesmo tempo, também é importante mencionarmos como o desenvolvimento da inteligência artificial (IA), especialmente os LLM (*large language models*), como ChatGPT, Gemini (antigo Bard) e outros, está transformando a forma como os dados são processados, armazenados e utilizados.

Modelos de IA, que utilizam grandes volumes de dados para "aprender", apresentam novos desafios à proteção da privacidade, particularmente quando informações pessoais e processuais públicas são integradas em seus sistemas. Ao contrário da simples desindexação de conteúdo em motores de busca tradicionais, em que links podem ser removidos da internet (mesmo que o discurso soe mais simples do que o que a prática nos mostra), fazer com que uma IA "esqueça" informações já absorvidas é uma tarefa tecnicamente difícil, senão impossível. Esse dilema abre um novo campo de discussão sobre o direito ao esquecimento e a persistência de dados em sistemas de IA.

O presente artigo examina a complexa questão da responsabilidade civil por divulgar informações processuais públicas, com base na análise da decisão do STF no Tema 1141, e faz um contraponto à luz dos desafios impostos pela popularização da IA generativa. O objetivo é analisar como a desinformação jurídica pode ser amplificada pela tecnologia, e como o direito ao esquecimento e a desindexação de conteúdo são conceitos que,

embora funcionem na web, se tornam muito mais complicados no contexto de dados massivos utilizados para treinamento de tais tecnologias. Ao final, o artigo propõe uma reflexão sobre a necessidade de novas regulamentações que equilibrem o direito à privacidade com o uso crescente de dados em sistemas de IA.

**O risco de desinformação**

Embora a publicidade processual tenha o intuito de promover a transparência, a ampliação da acessibilidade às informações judiciais através de plataformas digitais apresenta um novo desafio: o risco de desinformação jurídica. Quando informações processuais são publicadas de maneira descontextualizada ou simplificada, o público em geral pode tirar conclusões errôneas sobre o caso ou sobre as partes envolvidas.

Petições avulsas, por exemplo, são capazes de distorcer completamente a narrativa de um processo, assim como decisões que eventualmente sejam reformadas por instâncias superiores. Essa falta de contexto, quando somada à rápida disseminação de informações na internet e até mesmo ao caráter cada vez mais permanente que assumem, pode ser um potencializador da desinformação.

Como indicado na própria inicial do processo que deu origem ao Tema 1141, exemplos claros dessa problemática podem ocorrer em processos trabalhistas e criminais, nos quais a divulgação pública pode prejudicar as partes – mesmo que outras situações possam ser tão delicadas quanto, mesmo que em outros âmbitos, como aquelas envolvendo doenças ou questões íntimas. Aqui, cabe menção a um caso de um famoso ator brasileiro que acionou o Judiciário para implantação de prótese peniana, fato amplamente divulgado na mídia assim que o sigilo foi removido pelo juiz do processo (Bittencourt, 2017).

Especificamente em paralelo ao caso do Tema 1141, podemos pensar em trabalhadores que movem ações trabalhistas e como eles podem enfrentar dificuldades na busca de emprego devido à

exposição de seu processo (Redação STF, 2021). A publicação dessas informações, apesar de legal, pode afetar a reputação do reclamante, prejudicando suas oportunidades de emprego. Isso levanta o questionamento de até que ponto a publicidade processual deve prevalecer sobre a proteção à privacidade e à dignidade dos envolvidos – e, talvez, até mesmo se tal fator deve ser ponto de consideração e de discussão por parte dos próprios profissionais envolvidos no ajuizamento de ações do tipo.

Além disso, o crescimento de buscadores e plataformas como Escavador e Jusbrasil, que facilitam a pesquisa por informações processuais públicas, amplifica o impacto dessa exposição. Sabe-se que tais plataformas especializadas possuem certas barreiras que limitam alguns detalhes aos usuários pagantes, o que cabe mais como curiosidade do que, propriamente, como solução ou medida eficaz contra a publicidade desmedida.

Mesmo com tais barreiras, parece seguro afirmarmos que a amplificação digital ocorre porque esses sistemas permitem o acesso fácil e rápido a processos que, embora públicos, poderiam passar despercebidos em outros tempos, nos quais as consultas judiciais não eram tão acessíveis. A combinação de grande acessibilidade e ferramentas de busca robustas pode, inadvertidamente, alimentar um ciclo de desinformação ou de invasão de privacidade.

O risco de desinformação jurídica aumenta quando o público tem acesso a informações processuais sem o devido entendimento dos detalhes e das particularidades do caso. Como muitas informações jurídicas são técnicas e complexas, bem como necessitam de vários desdobramentos e documentos para total compreensão das narrativas, interpretações incorretas podem se tornar comuns.

Além disso, uma vez que essas informações estão publicamente disponíveis e integradas nos sistemas de busca, torna-se difícil controlar o uso que será feito delas. Não existe uma garantia de que a publicação inicial dessas informações seja acompanhada de correções ou atualizações quando novas decisões

ocorrerem no processo. Isso torna a desinformação persistente e potencialmente danosa a longo prazo.

Cabem aqui algumas reflexões sobre a persistência desse tipo de conteúdo no ambiente digital. A desindexação de conteúdo e o ato de "pedir remoção da internet", comuns em ações do tipo, muitas vezes são confundidos, mas têm implicações muito diferentes. A desindexação apenas retira um link dos resultados dos motores de busca, deixando o conteúdo intacto e acessível apenas em sua fonte original. Por sua vez, pedir a "remoção do conteúdo da internet" é um conceito vago e, na prática, muitas vezes ineficaz.

Remover completamente algo da internet implicaria não apenas a exclusão do conteúdo do site original, mas também a eliminação de qualquer cópia em cache, repositórios de arquivos e redes sociais que o tenham replicado. Isso torna o pedido de remoção demasiadamente amplo e difícil de ser cumprido, já que mesmo que o conteúdo seja removido de uma plataforma, ele pode reaparecer em outra que já tenha armazenado ou redistribuído essa informação – sem contar as réplicas "offline" ou físicas.

A persistência dos dados na IA amplia esse problema. Mesmo que o conteúdo seja desindexado ou removido de algumas fontes, se ele foi utilizado para treinar modelos de IA, seus efeitos provavelmente continuarão a ser refletidos nas respostas e decisões geradas por esses algoritmos, pois os dados assimilados durante o treinamento não podem ser simplesmente "desaprendidos". Isso revela quão limitada é a eficácia de pedir a remoção de conteúdo no atual contexto digital.

**O papel dos provedores de internet**

Com o aumento da digitalização de dados judiciais, plataformas de busca e serviços de indexação, ao mesmo tempo que acabaram se tornando tecnologias indispensáveis, também são centro de debates sobre responsabilidade civil e privacidade, especialmente quando tais informações podem causar danos à

reputação e à vida privada dos envolvidos, mesmo que em processos públicos.

No caso discutido no Tema 1141, um dos pontos cruciais é a falta de obrigação jurídica clara para que esses provedores removam informações processuais publicadas que não estão sob segredo de justiça. Como não há uma exigência legal explícita de exclusão de conteúdos processuais, essas plataformas podem manter as informações disponíveis publicamente por tempo indefinido, o que amplia o risco de danos às partes.

Mesmo que alguns dispositivos legais versem sobre o tema, a discussão ainda é complexa. O Marco Civil da Internet (Brasil, 2014b), por exemplo, possui um tópico específico sobre "Responsabilidade por Danos Decorrentes de Conteúdo Gerado por Terceiros" (Seção III), enquanto a Lei Geral de Proteção de Dados Pessoais (LGPD) elenca como fundamentos da disciplina da proteção de dados pessoais, "o respeito à privacidade", "a liberdade de expressão, de informação, de comunicação e de opinião" e "a inviolabilidade da intimidade, da honra e da imagem" (Brasil, 2018, Art. 2º).

Os provedores de internet frequentemente argumentam que estão apenas cumprindo o papel de facilitar o acesso público à informação, conforme previsto nos princípios constitucionais de publicidade processual e transparência. A tese de que essa atividade é lícita baseia-se no fato de que as informações processuais são publicamente acessíveis nos órgãos oficiais do Poder Judiciário e que a divulgação dessas informações atende ao exercício regular de direito de informar o público.

Em contraponto, situações específicas apontam para incompatibilidade, mesmo que indireta e apenas reflexa, de outras normativas, como a Resolução nº 139 do Conselho Superior da Justiça do Trabalho (CSJT). Ela dispõe sobre medidas a serem adotadas pelos Tribunais Regionais do Trabalho para impedir ou dificultar a busca de nome de empregados com o fim de elaboração de "listas sujas" (Brasil, 2014a).

Contudo, um dos pontos de crítica reside no fato de que essas informações, quando disponibilizadas de forma descontextualizada e amplamente acessíveis, podem causar dano moral ou prejuízos pessoais às partes envolvidas nos processos, especialmente em questões trabalhistas e criminais – além de outros como a falta de autorização para veiculação de notícias sobre os casos.

A ausência de uma legislação clara que regule a responsabilidade dos provedores pela manutenção ou remoção dessas informações processuais públicas cria um vácuo jurídico que alimenta os conflitos em torno da proteção à privacidade, conforme indicado até mesmo pelo reconhecimento de repercussão geral no caso.

Mais do que isso, a falta de obrigação de remoção é particularmente problemática no ambiente digital, onde, conforme já mencionado, as informações são amplamente replicadas e podem ser acessadas por meio de várias plataformas e motores de busca.

No contexto da responsabilidade civil, parece ser essencial a discussão sobre se os provedores de internet devem ser obrigados a adotar políticas de remoção ou restrição de acesso a informações processuais, particularmente quando estas podem causar danos significativos, bem como se isso é tecnicamente possível e se é necessária regulamentação legislativa específica sobre o tema – pensando até mesmo na regulação de inteligências artificiais.

**A decisão do STF e o Tema 1141**

O STF, em maio de 2021, reconheceu a repercussão geral da questão constitucional discutida no Tema 1141, que trata da responsabilidade civil pela disponibilização de informações processuais publicadas na internet. Essa questão levanta a necessidade de uniformizar o entendimento jurídico em âmbito nacional, estabelecendo se a divulgação dessas informações, desde que não estejam sob segredo de justiça e não haja uma obrigação jurídica de removê-las, deve ou não ser considerada legítima.

A repercussão geral significa que a decisão tomada pelo STF não afetará apenas o caso concreto discutido no recurso extraordinário com agravo (ARE 1307386), mas será aplicada de forma abrangente a todos os casos semelhantes no Brasil, que ficam suspensos até o julgamento do *leading case* (Minas Gerais, 2021). Isso ressalta a importância do julgamento, já que a tese jurídica que será firmada terá impacto sobre todos os processos judiciais que tratam da divulgação de informações processuais sem segredo de justiça em plataformas digitais.

**Repercussão geral e uniformização nacional**

A repercussão geral reconhecida pelo STF reforça a necessidade de se estabelecer uma tese jurídica que abranja todo o território nacional, evitando decisões conflitantes entre os tribunais estaduais/federais. Antes da intervenção do STF, a questão foi discutida no âmbito do Tribunal de Justiça do Rio Grande do Sul (TJ-RS), que acatou, em 1ª instância, a tese defensiva das rés. No entanto, essa decisão gerou efeitos restritos à jurisdição do TJ-RS.

O STF, ao reconhecer a importância constitucional da questão, busca criar uma uniformização nacional da jurisprudência, garantindo isonomia e segurança jurídica em todo o país, como um marco para definir até que ponto plataformas digitais podem divulgar informações processuais sem que isso resulte em danos às partes envolvidas, e se há um limite para essa divulgação no que se refere ao direito à privacidade.

**Análise da decisão do STF**

Um dos principais desafios da decisão do STF será equilibrar dois direitos fundamentais: o direito à informação e a transparência processual em contraponto ao direito à privacidade e à proteção da imagem das partes envolvidas.

O relator do caso, o Ministro Luiz Fux, destacou a importância de o STF analisar o alcance da publicidade processual no ambiente

digital, onde as informações podem ser disseminadas rapidamente e de forma irreversível. Fux argumentou que a decisão do STF deve levar em consideração o impacto da tecnologia no direito à privacidade e na forma como as informações são consumidas e interpretadas pelo público.

Cabe aqui a simples menção de que tanto a inicial como a decisão pela repercussão geral são anteriores à popularização da IA generativa, o que justifica a ausência de discussão sobre remoção de conteúdos do tipo das bases de dados usados para treinamento de tais tecnologias.

**Direito ao esquecimento vs. Desindexação e modelos de IA**

A decisão do STF no Tema 1141 sobre a responsabilidade civil pela divulgação de informações processuais públicas traz à tona um debate mais amplo sobre o direito ao esquecimento e a desindexação de dados no contexto digital. O direito ao esquecimento, consolidado pela jurisprudência europeia (Wolford, [s.d.]) e com inúmeros casos concretos no Direito brasileiro, permite que indivíduos, na prática, solicitem a remoção de informações pessoais irrelevantes ou prejudiciais, principalmente quando elas não são mais pertinentes para o público. No entanto, com o advento da inteligência artificial e a forma como esses dados são processados e utilizados, surgem desafios adicionais, pois "esquecer" informações em IA é tecnicamente mais complexo do que simplesmente desindexar conteúdo de uma plataforma de busca.

**Direito ao Esquecimento**

O direito ao esquecimento tem sua importância sempre lembrada em casos nos quais cidadãos solicitam a remoção de *links* e informações sobre si mesmos que não sejam mais relevantes ou que prejudiquem sua reputação. Esse direito visa proteger a privacidade e o direito à imagem, equilibrando o direito à informação com o direito de as pessoas não serem constantemente

associadas a eventos ou informações passadas que já perderam relevância. Esse mecanismo é importante para limitar a exposição prolongada de dados pessoais na internet, especialmente em casos onde a permanência dessas informações pode causar danos injustificados.

Apesar da importância e da já apontada pluralidade de menções legislativas sobre o assunto, cabe aqui menção ao "Tema 786 - Aplicabilidade do direito ao esquecimento na esfera civil quando for invocado pela própria vítima ou pelos seus familiares", em que foi definido, em 2021, pela incompatibilidade de direito ao esquecimento com os preceitos da Constituição, em caso originalmente sobre a repercussão midiática de crime brutal contra uma familiar dos requerentes, quase 50 anos depois do ocorrido (Brasil, 2016; Szaniawski, 2021).

> É incompatível com a Constituição a ideia de um direito ao esquecimento, assim entendido como o poder de obstar, em razão da passagem do tempo, a divulgação de fatos ou dados verídicos e licitamente obtidos e publicados em meios de comunicação social analógicos ou digitais. Eventuais excessos ou abusos no exercício da liberdade de expressão e de informação devem ser analisados caso a caso, a partir dos parâmetros constitucionais -especialmente os relativos à proteção da honra, da imagem, da privacidade e da personalidade em geral - e as expressas e específicas previsões legais nos âmbitos penal e cível (Rio de Janeiro, 2022, p. 329).

Tal contraponto parece indicar a pluralidade de ângulos sobre os quais a temática pode ser analisada, bem como a importância do tema.

**Dificuldade de "Esquecer" dados em modelos de IA**

Além da análise da cobertura midiática ou da simples reprodução de dados processuais públicos, quando tratamos de inteligência artificial, o conceito de "esquecer" informações torna-se significativamente mais complicado. Modelos de IA são treinados

com grandes volumes de dados, incluindo informações processuais, pessoais e outros conteúdos amplamente acessíveis. Esses dados são integrados diretamente no processo de aprendizado da máquina, o que significa que, uma vez absorvidos, eles se tornam parte do funcionamento do modelo.

Ao contrário da desindexação de conteúdo nos mecanismos de busca, que remove links de acesso a informações públicas, e até mesmo da remoção do conteúdo da internet, por mais genérico que isso seja, a IA não pode simplesmente "desaprender" informações da mesma maneira. O aprendizado da IA é baseado em um processo acumulativo, no qual os dados alimentam a tomada de decisões futuras do algoritmo. Portanto, mesmo que uma informação seja removida da internet, se ela já foi utilizada no treinamento de um modelo de IA, é praticamente impossível garantir que os impactos desse dado sejam completamente eliminados.

Por exemplo, o caso recente de um médico erroneamente acusado de crimes em uma resposta gerada pela IA do Bing, da Microsoft, exemplifica esse problema. A informação havia sido indexada corretamente, mas a IA replicou erroneamente o caso, que tratava originalmente de um médico que era um dos responsáveis pela análise de denúncias de assédios contra outros médicos. Em uma resposta sobre o autor, a IA replicou que ele seria um dos assediadores, e não um dos responsáveis pela investigação dos acusados (Fagundes, 2023; Santiago, 2023).

Apesar da correção, o que garante que o conteúdo foi "desindexado" da base de treinamento? É possível explicarmos o que acontece com modelos como os *large language models*, que absorvem conteúdo massivo e aprendem a replicar padrões?

Esse recente caso parece demonstrar como a desinformação pode ser amplificada e persistir em sistemas de IA, mesmo após correções ou remoções, se é que possíveis.

**Desindexação de conteúdo e IA**

A desindexação de conteúdo é um processo eficaz (em teoria) em motores de busca, mas quando se trata de IA, a questão parece mais complexa. Nos modelos de IA, as informações não são simplesmente armazenadas como *links* ou arquivos que podem ser removidos. Elas são incorporadas aos algoritmos que alimentam o aprendizado e a tomada de decisão do sistema. Uma vez que os dados são processados e utilizados no treinamento, eles se tornam parte integrante do funcionamento do modelo (Snyder, 2024).

Portanto, o desafio de "esquecer" dados em IA levanta uma questão crucial: como garantir a privacidade e o direito ao esquecimento em um contexto no qual a remoção de dados não é tão simples (se é que foi simples algum dia)? Mesmo com o início de discussões sobre o uso de dados em IA propondo soluções como a exigência de transparência no processo de treinamento dos modelos e a possibilidade de 'marcar' dados que não podem ser utilizados, ainda parecem necessárias novas regulamentações específicas para a IA, capazes de lidar com a persistência de dados pessoais em modelos de aprendizado de máquina.

Se a remoção ou desindexação de informações na internet pode ser realizada, a IA ainda parece carecer de ferramentas adequadas para remover informações previamente absorvidas e também de comprovação de tais remoções, criando um novo obstáculo para a proteção da privacidade no ambiente digital.

**Reflexões finais**

A discussão sobre o Tema 1141 do STF é um marco, pois aborda especificamente a questão da divulgação de informações processuais públicas, equilibrando o direito à informação com os direitos à privacidade e à imagem. No entanto, essa etapa inicial, onde foi reconhecida a repercussão geral, resolve apenas uma parte do quebra-cabeça. Parece que a questão levantada abrirá caminho para novos debates: qual será a próxima discussão sobre o tema?

Ao focar nos processos públicos, o STF reconheceu que a questão envolve o princípio da transparência processual, ao mesmo

tempo em que desafia os limites da responsabilidade civil das plataformas digitais. Provedores como Google e Escavador podem disponibilizar informações processuais que não tramitem em segredo de justiça, mas a decisão sobre até que ponto essas plataformas podem ser responsabilizadas por eventuais danos morais ainda precisa ser determinada pela corte.

A tese a ser firmada terá grande impacto na forma como as plataformas devem lidar com a divulgação desses dados. Embora a publicidade processual seja um princípio constitucional, as implicações tecnológicas e o uso generalizado de plataformas digitais tornam esse equilíbrio mais complexo. O STF precisará decidir se os provedores de internet devem ser responsabilizados quando a divulgação de informações processuais públicas prejudicar a reputação ou a imagem de uma pessoa, e até que ponto esses provedores têm o dever de remover ou desindexar informações, a fim de proteger os direitos individuais.

A repercussão geral reconhecida no Tema 1141 sinaliza que questões como a manutenção de dados na internet e os pedidos de remoção ou desindexação estão longe de serem resolvidas. A responsabilidade das plataformas, especialmente em relação a dados públicos, será uma discussão contínua. À medida que o julgamento avançar, será fundamental discutir o papel dessas plataformas na proteção da privacidade e na responsabilização por danos morais, equilibrando os direitos à informação e à privacidade.

Essas reflexões mostram que, embora o Tema 1141 aborde a questão da publicidade processual, novas frentes jurídicas surgirão, como o tratamento de dados sensíveis e a responsabilidade das plataformas por manter informações disponíveis de maneira pública e acessível.

No contexto do direito ao esquecimento, uma nova discussão pode surgir em torno da removibilidade real de dados na internet, indo além da desindexação e tocando na persistência de informações que continuam acessíveis em sistemas descentralizados ou em arquivos digitais de terceiros, e até mesmo

em ferramentas que permitem visualizar versões antigas de páginas de websites, como o Wayback Machine – será que a internet, do modo que ela se apresenta hoje, é compatível com o modo que pensamos a responsabilização e a remoção de conteúdo?

Essas reflexões mostram que, enquanto o tema atual é uma discussão sobre processos públicos, novas frentes jurídicas surgirão, como o tratamento de dados sensíveis e a legitimidade do uso de informações pessoais em contextos tecnológicos e comerciais, ampliando ainda mais o debate sobre privacidade e direitos de personalidade no contexto digital.

Quadro sinóptico do ARE 1307386

| |
|---|
| **1 - Qual o pedido feito na ação? Ou seja, quais foram os elementos fáticos e legais? Quem propôs a ação?**<br>A ação foi proposta por um trabalhador contra os sites Google e Escavador. O requerente havia movido uma reclamação trabalhista e, posteriormente, processou os sites por divulgar informações sobre a reclamação. Ele alegou que a divulgação estava prejudicando sua reputação e impedindo que potenciais empregadores o contratassem, temendo futuros processos trabalhistas. O trabalhador solicitou que as plataformas removessem as informações e pagassem uma indenização por danos morais, alegando que a publicidade processual estava afetando sua vida profissional. A base legal do pedido envolvia a proteção dos direitos de personalidade, incluindo privacidade e imagem, em confronto com o direito à informação pública. |
| **2 - Qual a efetiva decisão da Corte? A Corte (STF/TCF) privilegia a liberdade de expressão ou os direitos da personalidade?**<br>O Supremo Tribunal Federal (STF) reconheceu a repercussão geral do caso, ainda sem uma decisão final sobre a tese jurídica. Até o momento, a Corte tem privilegiado o direito à informação pública e a liberdade de expressão, argumentando que a divulgação de informações processuais, desde que não estejam sob segredo de justiça, é legítima. A decisão do STF abordará se os provedores de internet têm responsabilidade pela remoção dessas informações e se o direito à |

| |
|---|
| privacidade e à imagem prevalece sobre a transparência processual no contexto digital. |
| **3 - As Cortes utilizam o princípio ou critério da proporcionalidade como método de solução dos conflitos entre a liberdade de expressão e os direitos de personalidade na rede?**<br>No contexto jurídico brasileiro, nenhum direito é absoluto, especialmente quando se trata de conflitos entre a liberdade de expressão e os direitos da personalidade, como a privacidade e a proteção da imagem. O Supremo Tribunal Federal (STF) frequentemente aplica o princípio da proporcionalidade para equilibrar esses direitos em situações de conflito. A ideia central é que, ao garantir um direito, como o da liberdade de expressão, é preciso evitar que esse direito comprometa de forma desproporcional outros direitos fundamentais.<br>No caso do Tema 1141, que ainda será julgado pelo STF, a Corte deverá aplicar a proporcionalidade para avaliar se o direito à informação pública pode ser exercido sem causar danos desproporcionais aos direitos de privacidade das partes envolvidas. Esse julgamento será essencial para definir os limites da responsabilidade dos provedores de internet que divulgam informações processuais públicas.<br>Já no Tema 786, o STF decidiu que o direito ao esquecimento é incompatível com a Constituição, ou seja, não é possível impedir a divulgação de fatos ou dados verídicos e obtidos licitamente, mesmo com o passar do tempo. A liberdade de expressão e o direito à informação prevaleceram, mas a Corte deixou claro que eventuais excessos no uso desses direitos podem ser analisados caso a caso, com base em proteções constitucionais como a honra e a imagem<br>Esses temas mostram que o STF, ao tratar dessas questões, reforça o entendimento de que não há direitos absolutos: todos devem ser ponderados conforme o caso, levando em conta as consequências e impactos sobre os direitos das outras partes envolvidas. |

Fonte: Quadro produzido pelos autores.

**Conclusão**

A discussão sobre a divulgação de informações processuais públicas, como no Tema 1141 do STF (ARE 1307386), apresenta um ponto crucial para o equilíbrio entre o direito à informação e os direitos à privacidade e à imagem. A ação proposta por uma trabalhadora contra os sites Google e Escavador, que publicaram informações sobre um processo trabalhista, coloca em evidência os desafios de garantir a transparência processual sem causar danos morais ou prejuízos à reputação das partes envolvidas.

Embora o STF tenha reconhecido a repercussão geral, ainda não há uma decisão definitiva sobre o mérito da questão. A Corte deverá decidir se os provedores de internet devem ser responsabilizados pela manutenção ou remoção de informações processuais publicadas, especialmente quando essas informações podem impactar a vida privada e profissional de uma pessoa. A aplicação do princípio da proporcionalidade será central para balancear esses direitos em conflito, sem que nenhum deles prevaleça de forma absoluta.

O julgamento do Tema 1141 será fundamental para estabelecer uma tese jurídica vinculante para todos os casos semelhantes no Brasil, e poderá redefinir os limites da responsabilidade civil das plataformas digitais no que diz respeito à divulgação de informações processuais.

A discussão coloca em perspectiva a necessidade de novas regulamentações para lidar com as consequências da exposição de dados pessoais na era digital, seja por descontextualização ou pelo uso de inteligências artificiais, por exemplo. Isso exige uma reflexão mais profunda sobre as implicações da permanência de dados e as soluções jurídicas que poderão ser adotadas para proteger a privacidade e garantir a responsabilização adequada dos provedores de internet.

## Referências


BITTENCOURT, J. Após 3 anos em segredo de justiça, processo de Frota para obter prótese peniana se torna público. **Revista Fórum**, 13 nov. 2017. Disponível em: <https://revistaforum.com.br/brasil/2017/11/13/apos-anos-em-segredo-de-justia-processo-de-frota-para-obter-protese-peniana-se-torna-publico-24118.html>. Acesso em: 14 out. 2024.

BRASIL. Conselho Nacional de Justiça. **Resolução nº 121**, de 5 de outubro de 2010. Dispõe sobre a divulgação de dados processuais eletrônicos na rede mundial de computadores, expedição de certidões judiciais e dá outras providências. Brasília, 5 out. 2010. Disponível em: <https://atos.cnj.jus.br/atos/detalhar/atos-normativos?documento=92>. Acesso em: 14 out. 2024.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, 5 out. 1988. Disponível em: <https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 14 out. 2024.

BRASIL. Conselho Superior da Justiça do Trabalho. **Resolução CSJT n.º 139**, de 24 de junho de 2014. Brasília, 24 jun. 2014a. Disponível em: <https://hdl.handle.net/20.500.12178/39800>. Acesso em: 14 out. 2024.

BRASIL. Supremo Tribunal Federal. **ARE 1307386**. Tema 1141 - Responsabilidade civil por disponibilização na internet de informações processuais publicadas nos órgãos oficiais do Poder Judiciário, sem restrição de segredo de justiça ou obrigação jurídica de remoção. Brasília, 19 jan. 2021. Disponível em: <https://portal.stf.jus.br/jurisprudenciarepercussao/verAndamentoProcesso.asp?incidente=6087432&numeroProcesso=1307386&classeProcesso=ARE&numeroTema=1141>. Acesso em: 14 out. 2024.

BRASIL. Supremo Tribunal Federal. **Lei nº 12.965**, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, 23 abr. 2014b. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 14 out. 2024.

BRASIL. Supremo Tribunal Federal. **Lei nº 13.709**, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, 14 ago. 2018. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 14 out. 2024.

BRASIL. Supremo Tribunal Federal. **RE n° 1010606**. Tema 786 - Aplicabilidade do direito ao esquecimento na esfera civil quando for invocado pela própria vítima ou pelos seus familiares. Brasília, 14 nov. 2016. Disponível em: <https://portal.stf.jus.br/jurisprudenciaRepercussao/verAndamentoProcesso.asp?incidente=5091603&numeroProcesso=1010606&classeProcesso=RE&numeroTema=786>. Acesso em: 14 out. 2024.

FAGUNDES, J. Erro impactante da IA: médico vítima de falsas acusações de 100 assédios, enfrentando desafios profissionais e pessoais. **Jusbrasil**, 2023. Disponível em: <https://www.jusbrasil.com.br/noticias/erro-impactante-da-ia-medico-vitima-de-falsas-acusacoes-de-100-assedios-enfrentando-desafios-profissionais-e-pessoais/1872586501>. Acesso em: 14 out. 2024.

MINAS GERAIS. Tribunal de Justiça do Estado de Minas Gerais. **Reconhecimento de Existência de Repercussão Geral**, 07 mai. 2021. Responsabilidade civil por disponibilização na internet de informações processuais publicadas nos órgãos oficiais do Poder Judiciário, sem restrição de segredo de justiça ou obrigação jurídica de remoção. Disponível em: <https://www.tjmg.jus.br/portal-tjmg/jurisprudencia/recurso-repetitivo-e-repercussao-geral/responsabilidade-civil-por--na-internet-de-informacoes-processuais-publicadas-nos-orgaos-oficiais-do-poder-judiciario-sem-restricao-de-segredo-de-justica-ou-obrigacao-juridica-de-remocao-tema-1141-stf.htm>. Acesso em: 14 out. 2024.

WOLFORD, B. Everything you need to know about the "Right to be forgotten". **GDPR.EU**, [s.d.]. Disponível em: <https://gdpr.eu/right-to-be-forgotten/>. Acesso em: 14 out. 2024.

REDAÇÃO STF. STF discutirá responsabilização por divulgação de informações processuais em sites na internet. **Supremo Tribunal Federal (STF)**, Brasília, 10 mai. 2021. Disponível em: <https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=465620&ori=1>. Acesso em: 14 out. 2024.

RIO DE JANEIRO. Ministério Público do Estado do Rio de Janeiro. **RE nº 1010606**, Rio de Janeiro. 11 fev. 2021. *In*: Revista do Ministério Público do Estado do Rio de Janeiro, nº 84, p. 327-563, abr./jun. 2022. Disponível em: <https://www.mprj.mp.br/servicos/revista-do-mp/revista-84/artigo-das-pags-327-563>. Acesso em: 14 out. 2024.

SANTIAGO, A. IA erra e acusa médico de 100 assédios: 'Quase acabou com uma carreira'. **UOL**, Florianópolis, 22 jun. 2023. Disponível em: <https://www.uol.com.br/tilt/noticias/redacao/2023/06/22/medico-acusado-assedio-erro-ia-bing-microsoft.htm>. Acesso em: 14 out. 2024.

SNYDER, A. Machine forgetting: How difficult it is to get AI to forget. **Axios**, 12 jan. 2024. Disponível em: <https://www.axios.com/2024/01/12/ai-forget-unlearn-data-privacy>. Acesso em: 14 out. 2024.

SZANIAWSKI, E. O Supremo Tribunal Federal e o julgamento do caso Aída Curi - Parte 1. **Consultor Jurídico (Conjur)**, 26 abr. 2021. Disponível em: <https://www.conjur.com.br/2021-abr-26/direito-civil-atual-supremo-tribunal-federal-julgamento-aida-curi/>. Acesso em: 14 out. 2024.

# EIXO BANCO DE DADOS

# Acesso a informações nos bancos de dados da Receita Federal: governança de dados e privacidade

Carlo José Napolitano
Deborah Cunha Teodoro
Lucas Catib Laurentiis
Tatiana Stroppa

Este capítulo objetiva apresentar e analisar decisão proferida pelo Supremo Tribunal Federal no Recurso Extraordinário 673707, interposto pela empresa Rigliminas Distribuidora Ltda. Com sede em Belo Horizonte/MG, a sociedade empresária limitada iniciou suas atividades em 04 de novembro de 1993, exercendo o comércio atacadista de alimentos para animais, como rações e demais produtos alimentícios para cavalos, cães, gatos, peixes e hamsters. A empresa também atendia outros estabelecimentos comerciais de escala menor, *pet-shops*, propriedades com criação de animais e criadouros, encerrando as atividades por liquidação voluntária em 04 de maio de 2015 (CNPJ.info, 2024).

Como elementos fáticos e jurídicos da ação, tem-se que a empresa Rigliminas Distribuidora Ltda ajuizou *habeas data*, na primeira instância, com o intuito de obter todas as informações relativas a débitos constantes em seu nome, bem como de todos os pagamentos efetuados armazenados nas bases de dados de apoio ao controle da arrecadação federal utilizadas pela Secretaria da Receita Federal, em especial, no Sistema de Conta Corrente da *Receita Federal* - SINCOR. A empresa mineira pretendia averiguar a existência de pagamentos em duplicidade para quitação de impostos e contribuições federais controlados pelo órgão, a fim de utilizar eventuais créditos na compensação de débitos.

Inspirado pelas legislações de Portugal, Espanha e Estados Unidos, que desde os anos 1970 passaram a incluir o direito de

cidadãos acessarem dados pessoais em bancos de entidades governamentais, o *habeas data* surgiu no ordenamento jurídico brasileiro com a Constituição da República Federativa do Brasil de 1988. Previsto no artigo 5º, inciso LXXII, da CRFB/1988 e destinado a assegurar que um cidadão tenha acesso a dados e informações pessoais que estejam sob a posse do Estado brasileiro ou de entidades privadas que tenham informações de caráter público, este remédio constitucional contempla ao impetrante o direito de saber o que é de conhecimento do governo sobre ele, além de poder ser acionado para corrigir dados pessoais que estejam equivocados (Wald; Fonseca, 1998, p. 45).

Wald e Fonseca (1998, p. 49) alertam que o *habeas data* pode ser impetrado tanto por pessoa física quanto jurídica, justificando que "não há motivos para excluir as pessoas jurídicas se a Constituição não o fez. Assim, da mesma forma como podem impetrar mandado de segurança, as pessoas jurídicas também podem impetrar *habeas data*".

Segundo Wald e Fonseca (1998, p. 47), a inclusão do *habeas data* na CRFB/1988 foi motivada por um fator político: facilitar o acesso aos registros do antigo Sistema Nacional de Informações (SNI), banco de dados mantido pelo regime militar (1964-1985), que reunia diversas informações sobre os cidadãos brasileiros. Para disciplinar o instituto, foi editada a Lei 9.507, de 12 de novembro de 1997**,** que regula o direito de acesso a informações e disciplina o rito processual do *habeas data*.

A súmula 2 do STJ determina que o *habeas data* é cabível somente nos casos em que o cidadão tiver solicitado, anteriormente, a um órgão público, o acesso a dados pessoais, obtendo a negativa desse órgão. Sem essa recusa prévia, o pedido é negado: "Não cabe o habeas data (CF, art. 5., LXXII, letra "a") se não houve recusa de informações por parte da autoridade administrativa." (STJ, 2024, p. 1).

Portanto, primeiramente, o interessado deve apresentar um pedido de acesso aos dados para o órgão público, que dispõe de 48 horas para análise. Após esse período, o cidadão é informado, em 24 horas, da decisão do órgão. Se recusado o requerimento, cabe o

*habeas data*. Em casos de inexatidão de dados, deve ser feita uma petição com documentos que comprovem o problema. Apresentada a petição, o órgão tem dez dias para corrigir os dados inexatos e comunicar a correção ao requerente.

No *habeas data* impetrado pela Rigliminas Distribuidora Ltda, o juiz de primeiro grau julgou improcedente a ação, decisão confirmada pelo Tribunal Regional Federal da 1ª Região, por entender que o registro indicado não se enquadra na hipótese de cadastro público.

Assim foi ementado o Acórdão do TRF da 1ª Região:

> HABEAS DATA. PEDIDO ÀS INFORMAÇÕES RELATIVAS A TODAS AS ANOTAÇÕES CONSTANTES DOS ARQUIVOS DA RECEITA FEDERAL. SINCOR. NÃO SE ENQUADRA NA HIPÓTESE DE CADASTRO PÚBLICO.
> I - O habeas data assegura o acesso a informações relativas à pessoa do impetrante, constantes de registros públicos ou banco de dados de entidades governamentais ou de caráter público (art. 5º, LXXII, "a", Constituição), afigurando-se, na espécie, inadequada a via eleita pelo impetrante para satisfazer sua pretensão de obter informações de dados relativos a terceiros.
> II - Apelação não provida.

No Recurso Extraordinário a empresa alegou violação ao artigo 5º, LXXII, "a", da CRFB/88, sustentando, em síntese, que é direito constitucional conhecer as anotações, informações e dados sobre pagamentos por ela implementados nos sistemas de apoio à arrecadação de tributos federais da Secretaria da Receita Federal do Brasil, de forma que exista transparência da atividade administrativa, principalmente com relação às informações que digam respeito ao próprio contribuinte.

Logo o pedido feito no recurso pela empresa recorrente baseou-se no artigo 5º, LXXII, "a" do texto Constitucional que dispõe:

> LXXII - conceder-se-á *"habeas-data":*
> a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público

A Secretaria da Receita Federal, em contrarrazões no RE, por sua vez, alegou que os cadastros e bases de dados de controle de pagamentos não se tratam de cadastros públicos, mas sistema de controle interno da Secretaria da Receita Federal do Brasil, o que inviabiliza a concessão do *habeas data.*

A Procuradoria-Geral da República manifestou-se pelo provimento do recurso extraordinário, aduzindo que a ausência de caráter público dos sistemas não impede o acesso a informações, portanto, não constitui argumento suficiente para indeferir o *habeas data*, já que o cadastro é mantido por uma entidade governamental. Dessa forma, o contribuinte tem o direito de obter informações contidas no SINCOR, com base no art. 5º, LXXII, "*a*", da CRFB/1988.

O Conselho Federal da Ordem dos Advogados do Brasil (CFOAB), na qualidade de interessado na causa (*amicus curiae*), conforme deferido pelo Relator Ministro Luiz Fux, em 05 de agosto de 2014, corroborou o direito constitucional postulado pela empresa RIGLIMINAS DISTRIBUIDORA LTDA com a alegação de que a administração pública não pode reter informação, recusando-se a repassá-la ao próprio contribuinte.

O Supremo Tribunal Federal, por unanimidade e nos termos do voto do Relator Ministro Luiz Fux, deu provimento ao Recurso Extraordinário, assentando a tese de que o *habeas data* é a garantia constitucional adequada para a obtenção, pelo próprio contribuinte, dos dados concernentes ao pagamento de tributos constantes de sistemas informatizados de apoio à arrecadação dos órgãos da administração fazendária dos entes estatais.

Na fundamentação da decisão do voto do Ministro Relator, dentre outros argumentos, aduz que "o *habeas data* é uma ação constitucional por meio da qual se visa garantir o acesso de uma

pessoa a informações **sobre ela** que façam parte de arquivos ou **bancos de dados** de entidades governamentais ou públicas".

Indica ainda que "Aos contribuintes foi assegurado o direito de conhecer as informações que lhes digam respeito em bancos de dados públicos ou de caráter público, em razão da necessidade de preservar o status de seu nome, planejamento empresarial, estratégia de investimento e, em especial, a recuperação de tributos pagos indevidamente, dentre outras. Consectariamente, estas informações não são de uso privativo do órgão ou entidade produtora ou depositária das informações, a Receita Federal do Brasil, mas dizem respeito ao próprio contribuinte."

A decisão menciona ainda que "o registro de dados deve ser entendido em seu sentido mais amplo, abrangendo tudo que diga respeito ao interessado, seja de modo direto ou indireto", bem como que "as informações fiscais conexas ao próprio contribuinte, se forem sigilosas, não importa em que grau, devem ser protegidas da sociedade em geral, segundo os termos da lei ou da constituição, mas não de quem a elas se referem, por força da consagração do direito à informação do art. 5º, inciso XXXIII, da Carta Magna, que traz como única ressalva o sigilo imprescindível à segurança da sociedade e do Estado, o que não se aplica no caso."

Reconhece e reafirma o caráter público dos bancos de dados da Receita Federal.

Com esses fundamentos, o STF dá provimento ao Recurso Extraordinário, concedendo o habeas data para a empresa recorrente.

Verifica-se que o STF, na decisão, reafirmou o direito à informação consagrado no texto constitucional (artigo 5º, XXXIII - Todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado), regulamentado pela Lei de Acesso à Informação – LAI, Lei 12.527/2011, proporcionando que a empresa contribuinte tivesse acesso a todos os seus dados constantes no

sistema da Receita Federal, privilegiando dessa forma o direito à informação do contribuinte.

Na ementa e no acórdão não há indicação da utilização do critério da proporcionalidade, como razão de decidir.

Contudo, no voto do Ministro Relator Luiz Fux, que foi acompanhado por unanimidade pelos demais ministros, verifica-se que houve a menção ao critério, nos seguintes termos "Por fim, os princípios da razoabilidade e da proporcionalidade são violados pelo próprio Estado através da administração fazendária ao não permitir ao contribuinte o acesso a todas as informações fiscais inerentes aos seus deveres e ao cumprimento de suas obrigações tributárias principais e acessórias, como sói ocorrer com o atual Centro Virtual de Atendimento da Receita Federal do Brasil/E-CAC."

De todo modo, a Corte não utilizou esse critério para a solução do conflito jurídico.

A Procuradoria-Geral da Fazenda Nacional (PGFN), após a decisão do STF, incluiu a questão na lista de temas com dispensa de contestar e/ou recorrer da Procuradoria-Geral, com a tese de que "o habeas data é a garantia constitucional adequada para a obtenção dos dados concernentes ao pagamento de tributos do próprio contribuinte constantes dos sistemas informatizados de apoio à arrecadação dos órgãos da administração fazendária dos entes estatais." (PGFN, 2016, p. 9).

Para a Procuradoria-Geral da Fazenda Nacional, o SINCOR registra os dados de apoio à arrecadação federal ao armazenar os débitos e créditos dos contribuintes, encartando-se, assim, "no conceito mais amplo de arquivos, bancos ou registro de dados, que devem ser entendidos em seu sentido mais lato, abrangendo tudo que diga respeito ao interessado, seja de modo direto ou indireto." (PGFN, 2016, p. 4).

A PGFN ratifica que pessoas jurídicas possuem legitimidade ativa para a impetração do *habeas data*, desde que preencham os requisitos exigidos, como as condições da ação e os pressupostos processuais, porque aos contribuintes foi assegurado o direito de conhecer as informações que lhes dizem respeito em bancos de dados

públicos ou de caráter público, visando a preservar, por exemplo, o *status* de seu nome, o planejamento empresarial, a estratégia de investimento e a recuperação de tributos pagos indevidamente. Tais informações se referem ao próprio contribuinte, não sendo de uso privativo do órgão ou entidade produtora ou depositária das informações, como, no caso, a Receita Federal.

Salienta a PGFN que os extratos atinentes às anotações constantes do SINCOR, como de quaisquer dos sistemas informatizados de apoio à arrecadação federal utilizados pela Receita Federal, no que tange aos pagamentos de tributos federais, não envolvem a hipótese de sigilo legal ou constitucional, posto que requerida pelo contribuinte sobre dados próprios. Portanto, tratando-se de informação subjetiva, ou seja, de dados pessoais relativos ao próprio requerente, não há como ser considerada comprometedora para a segurança da sociedade ou do Estado, razão pela qual não pode ser negada ao próprio requerente. (PGFN, 2016, p. 5).

Quadro sinóptico do RE 673707

| |
|---|
| **1 - Qual o pedido feito na ação? Ou seja, quais foram os elementos fáticos e legais? Quem propôs a ação?**<br>A ação, proposta pela empresa RIGLIMINAS DISTRIBUIDORA LTDA, tinha o objetivo de obter todas as informações relativas a débitos constantes em seu nome, bem como a todos os pagamentos efetuados que constassem das bases de dados de apoio ao controle da arrecadação federal utilizadas pela Secretaria da Receita Federal, em especial, do sistema SINCOR (Sistema de Conta Corrente da Receita Federal). A empresa apontava violação ao artigo 5º, LXXII, "a", da CRFB/88, sustentando que é direito constitucional conhecer as anotações, informações e dados sobre pagamentos por ela implementados nos sistemas de apoio à arrecadação de tributos federais da Secretaria da Receita Federal, de forma que exista transparência da atividade administrativa, principalmente, em relação a informações sobre o próprio contribuinte. |
| **2 - Qual a efetiva decisão da Corte? A Corte (STF/TCF) privilegia a liberdade de expressão ou os direitos da personalidade?** |

| |
|---|
| O STF deu provimento, por unanimidade, ao recurso extraordinário, assentando a tese de que o *habeas data* é a garantia constitucional adequada para a obtenção, pelo próprio contribuinte, dos dados concernentes ao pagamento de tributos constantes de sistemas informatizados de apoio à arrecadação dos órgãos da administração fazendária dos entes estatais. Assim, a Corte privilegia o acesso à informação pessoal, ao dar provimento ao RE 673707 com a tese de que "o *habeas data* é a garantia constitucional adequada para a obtenção dos dados concernentes ao pagamento de tributos do próprio contribuinte constantes dos sistemas informatizados de apoio à arrecadação dos órgãos da administração fazendária dos entes estatais." (BRASIL, p. 3). |
| **3- As Cortes utilizam o princípio ou critério da proporcionalidade como método de solução dos conflitos entre a liberdade de expressão e os direitos de personalidade na rede?**<br>Na ementa e no acórdão não há indicação da utilização do critério da proporcionalidade como razão de decidir, contudo, ao mencionar o voto do Ministro Relator Luiz Fux, acompanhado por unanimidade pelos demais ministros, no acórdão do RE 673707 (BRASIL, p. 24) que "os princípios da razoabilidade e da proporcionalidade são violados pelo próprio Estado, através da administração fazendária, ao não permitir ao contribuinte o acesso a todas as informações fiscais inerentes aos seus deveres e ao cumprimento de suas obrigações tributarias principais e acessórias, como ocorre com o atual Centro Virtual de Atendimento da Receita Federal do Brasil/E-CAC", verifica-se que houve a menção aos critérios da razoabilidade e da proporcionalidade como método de solução de conflitos entre direitos fundamentais. |

Fonte: Quadro elaborado pelos autores

## Referências

BRASIL. **Constituição da República Federativa do Brasil de 1988**, promulgada em 5 de outubro de 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 1 out. 2024.

BRASIL. **PGFN. NOTA PGFN/CRJ/Nº 801/2016, de 15 de agosto de 2016**. Registro 00202183/2016 Consulta CASTF – Lista de dispensa – RE 673.707 – MG. Disponível em: https://www.gov.br/receitafederal/pt-br/acesso-a-informacao/legislacao/decisoes-vinculantes-do-stf-e-do-stj-repercussao-geral-e-recursos-repetitivos/arquivos-e-imagens/nota-crj-801-2016.pdf. Acesso em: 3 out. 2024.

BRASIL. **Supremo Tribunal Federal. RE 673707**. Disponível em: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=9487405. Acesso em: maio de 2024.

Rigliminas Distribuidora LTDA. **CNPJ.info**. Disponível em: http://cnpj.info/Rigliminas-Distribuidora-Ltda. Acesso em: 20 jun. 2024.

Enunciados das Súmulas do STJ. **STJ – Superior Tribunal de Justiça**. Disponível em: https://www.stj.jus.br/docs_internet/jurisprudencia/tematica/download/SU/Verbetes/VerbetesSTJ_asc.pdf. Acesso em: 20 jun. 2024.

WALD, Arnold; FONSECA, Rodrigo Garcia da. O habeas data na Lei nº 9.507/97. In: **Revista do Ministério Público do Estado do Rio de Janeiro**, Rio de Janeiro, nº 7, p. 45-59, jan./jun. 1998.

# EIXO PROTEÇÃO DE DADOS

# Proteção de dados e os meios de telecomunicações na realidade alemã: uma análise de caso

Laura Santos Lopes
Luiz Henrique Ranzani
Sarah Thiemy Kawato dos Santos

## Introdução

O advento da internet e das telecomunicações, simultâneo a outros avanços tecnológicos significativos para a humanidade, indubitavelmente surgiram para facilitar a troca de informações e a disseminação de conhecimentos ao redor do mundo. Essas evoluções, no entanto, não surgiram livres de inquietações básicas e inerentes às discussões que fazem referência a direitos fundamentais, como o da privacidade. O cenário alemão aqui analisado ilustra bem como essas preocupações se movimentam na sociedade contemporânea ao traçar uma discussão acerca da regulamentação legal relativa à proteção de dados pelos meios de telecomunicações na realidade do país europeu.

A Diretiva 2006/24/CE do Parlamento Europeu, conhecida como Diretiva de Retenção de Dados, que mantém vinculação direta com o tema deste capítulo, foi uma alternativa de segurança adotada pela União Europeia (UE) em face das crescentes ameaças de ações terroristas postas em prática no solo dos países integrantes do bloco após o trágico atentado de 11 de setembro de 2001 nos Estados Unidos. Nesse ínterim, não é difícil constatar que houve a perpetração de uma vigilância preventiva por parte dos Estados-membros da UE - e a Alemanha não ficou isenta, pelo contrário, a república promulgou a Diretiva por meio de uma revisão da sua Lei de Telecomunicações, ação que, com o passar do tempo, passou a ser contestada em virtude do seu potencial de transgredir a

privacidade e proteção de dados dos cidadãos alemães (União Europeia, 2006).

O presente capítulo tem como escopo descrever e analisar um julgamento realizado pelo Tribunal Constitucional Alemão (TCF) de três casos, BvR 256, 263 e 586/08, os quais se concatenam intrinsecamente com a Diretiva 2006/24/CE e foram julgados em conjunto pela Corte no ano de 2010.

**BvR 256/08, 263/08 e 586/08**

O primeiro caso alemão, BvR 256/08, tem como cerne a contestação dos §§ 113a e 113b da Lei de Telecomunicações, ambos dispositivos cuja gênese foi o Art. 2, nº 6 da Lei de Revisão da Vigilância de Telecomunicações e Outras Medidas de Investigação Oculta e pela transposição da Diretiva 2006/24/CE de 21 de dezembro de 2007. De acordo com a alegação da parte reclamante do processo, os §§ 113a e 113b da Lei de Telecomunicações violam as garantias previstas nos artigos 10(1), 12(1), 14(1), 5(1) e 3(1) da Lei Fundamental.

O segundo caso, BvR 263/08, por sua vez, vai de frente ao conteúdo previsto nesta última lei revisora, já que os reclamantes argumentam que os §§ 113a e 113b da Lei de Telecomunicações e o § 100g do Código de Processo Penal estão em desacordo com as garantias dos artigos 1(1), 2(1), 10(1) e 19(2) da Carta Magna alemã. Por fim, o terceiro caso, BvR 586/08, parte do questionamento das disposições sobre retenção de dados da mesma legislação, por acreditarem que tal prática transgride os artigos 10(1), 2(1) e 1(1) da Constituição do país (Alemanha, 2010). Em síntese, a tríade de ações constrói referências contestatórias às disposições da Lei de Telecomunicações e do Código de Processo Penal, mais precisamente, aos §§ 113a e 113b da peça legislativa.

O polêmico § 113a (1) da referida Lei de Telecomunicações tem como objetivo obrigar que os prestadores de serviços de telecomunicação (chamadas telefônicas fixas ou de celulares, aplicativos de mensageria que funcionam via internet e afins)

retenham os dados de tráfego que contêm informações, como tempo gasto na comunicação pelos usuários e suas localizações, pelo período de seis meses. Além disso, tais dados devem ficar disponíveis para as autoridades alemãs, sendo sua exclusão imposta dentro de um mês após o término desse prazo pré-estabelecido (Alemanha, 2010). O mesmo parágrafo, porém, impede o acesso ao conteúdo das comunicações e aos dados dos sites acessados. A princípio, tal retenção de informações, e possível disponibilização delas às autoridades (mediante solicitação prévia), tem a finalidade de atender a medidas que mitiguem perigos à segurança e ordem pública, bem como auxiliar na persecução de crimes e infrações administrativas (Alemanha, 2010).

Em contrapartida, os artigos da Constituição que os reclamantes entendem como violados pela Lei de Telecomunicações garantem, no escopo dos direitos fundamentais, a privacidade do conteúdo das telecomunicações, assim como das informações que dizem respeito sobre as circunstâncias em que elas foram realizadas. Tal proteção é estipulada, inclusive, contra possíveis abusos advindos de autoridades públicas - uma prevenção à vigilância estatal extremada, vista em distopias de grande sucesso, como a experimentada no livro 1984, do escritor George Orwell (Orwell, 2009). Além da privacidade, o direito à autodeterminação informativa também é uma garantia presente nos artigos citados pelos reclamantes. Conforme tais alegações, o conhecimento, armazenamento ou processamento de dados de telecomunicações e de seus conteúdos podem ser entendidos como interferências diretas à plenitude dos direitos constitucionais garantidos, ou seja, como práticas inconstitucionais. Em síntese, pode-se afirmar, portanto, que a dialética aqui imposta pelos três casos contrapõe a proteção de dados *versus* a segurança pública.

No julgamento, os juízes consideram as queixas constitucionais bem fundamentadas e proferem decisão majoritária favorável à proteção de dados dos usuários de serviços de telecomunicações em detrimento da segurança pública, um dos alicerces causais da legislação contestada. Os magistrados, em

conformidade com a argumentação dos proponentes das ações, aduziram que os §§ 113a e 113b da Lei de Telecomunicações, que nasceram com a Lei que Revise a Legislação sobre Vigilância de Telecomunicações, violam o artigo 10(1) da Constituição e, em virtude dessa violação, determinaram a nulidade dos dispositivos - sem declarar, todavia, a inconstitucionalidade deles. Na mesma esteira, o § 100g(1), do Código de Processo Penal, também alterado pela lei revisora citada acima, foi outra peça determinada nula pelos julgadores, por transgredir o disposto no artigo 10(1) da Lei Fundamental, ao conceder permissão para obtenção de dados, seguindo o previsto no § 113a da Lei de Telecomunicações, e esbarrar no direito de privacidade dos cidadãos alemães.

Além disso, foi determinada a obrigação de exclusão, sem morosidade injustificada, dos dados de tráfego de telecomunicações solicitados por autoridades públicas, não enviados e mantidos pelos provedores sob seu escopo.

A opinião divergente do juiz Eichberger ainda presta o papel de elucidar como a discussão entre privacidade *versus* segurança pública é profunda e multifacetada. Ao contrário de seus colegas, o magistrado acredita que o fato de a retenção dos dados acontecer de maneira descentralizada, sendo realizada por vários prestadores de serviços privados, e não abranger o conteúdo das telecomunicações prova que tal prática de retenção não provoca qualquer efeito inibidor e maléfico à comunicação da população, sendo, assim, convergente com a Lei Básica. Eichberger, porém, teve sua tese derrotada (Alemanha, 2010).

O Tribunal Federal Alemão, ao justificar seu posicionamento, aplicou o princípio da proporcionalidade de modo a não sacrificar inteiramente nenhum dos lados postos em contraposição (Farias, 2004), conforme a sua delimitação clássica (Dimoulis; Martins, 2022), sendo subdividido em três etapas: adequação, necessidade e ponderação ou proporcionalidade em sentido estrito.

Antes de analisar a proporcionalidade, a Corte delimitou o âmbito protetivo, isto é, o conteúdo protegido do direito que foi violado. O direito à privacidade das telecomunicações, protegido

pelo art. 10(1) da Lei Fundamental, garante a proteção da transmissão de informações não físicas a destinatários individuais ou através de meios de telecomunicação, em face das autoridades públicas que eventualmente possam ter acesso a esse conteúdo. A proteção abrange não apenas o conteúdo propriamente dito, como também situações específicas relacionadas com a forma e a frequência da obtenção dos dados em questão. Ainda, inclui garantia de proteção em relação ao primeiro acesso das informações pelas autoridades públicas, bem como quanto ao processamento de dados realizados após a sua obtenção.

É interessante ressaltar que as partes haviam alegado também a ofensa ao direito à autodeterminação informativa, previsto no art. 2(1) e 1(1), mas o Tribunal concluiu que esse direito não seria aplicado ao caso concreto, por se tratar de um direito geral, se comparado com o direito à privacidade das telecomunicações, que traz regulamentos específicos cabíveis ao caso em questão.

Em seguida, identificou todas as situações que podem caracterizar uma interferência àquele direito, o que inclui a obtenção, armazenamento ou processamento de dados de telecomunicações por parte das autoridades públicas. Também configura uma interferência a coleta e o armazenamento de dados de telecomunicações, bem como a verificação cruzada com outros dados, a sua análise ou a sua posterior transferência a terceiros. Da mesma forma, obrigações impostas às empresas para a coleta de tais dados para fins de informar autoridades, também são consideradas intervenções.

Especificamente em se tratando da aplicação do princípio da proporcionalidade, tais interferências podem ser consideradas constitucionais se os seus propósitos forem legítimos e trouxerem algum benefício para o bem comum.

A Corte analisou separadamente as três normas cuja constitucionalidade foi questionada. Em termos gerais, os seus objetivos foram reputados legítimos, dentre os quais a promoção da segurança pública e a realização de tarefas de inteligência. Nesse sentido, ao aplicar a primeira fase do princípio da

proporcionalidade, considerou que se tratam de meios adequados para a garantia daqueles objetivos.

Em relação à segunda etapa, o TCF também considerou se tratar de medidas necessárias, considerando que inexistem meios menos restritivos possíveis para que tais bens jurídicos fossem protegidos sem que houvesse interferência tão ampla ao direito que se pretende proteger, e que fosse suficientemente apto a garantir a investigação necessária.

No entanto, alguns empecilhos ligados à proporcionalidade em sentido estrito foram encontrados para reputar as normas constitucionais. Em termos amplos, a Corte considerou que apesar dos dados armazenados se referirem essencialmente aos dados de tráfego, como a duração, conexões, localização, e não ao conteúdo propriamente dito, podem trazer amplas informações sobre os usuários, inclusive em relação a informações pessoais e íntimas. Dessa forma, a interferência à privacidade seria amplamente permitida, sem que houvesse garantias suficientes para proteger os dados obtidos.

Como consequência, haveria uma sensação de vigilância constante, inclusive gerando um aumento significativo da possibilidade de que indivíduos sejam investigados, ainda que critérios básicos para tanto não sejam cumpridos. Isto é, haveria um potencial abuso à proteção de dados, situação agravada ante a possibilidade de retenção de dados sem a ciência da pessoa que é investigada.

Diante disso, uma vez que estejam estabelecidos os propósitos para a coleta de dados, seria possível considerar as normas como proporcionais em sentido estrito, ou seja, constitucionais. No entanto, tanto a Lei de Telecomunicações como o Código de Processo Penal deixaram de identificar com clareza tais elementos. Por essas razões, na terceira fase da proporcionalidade (ponderação), o Tribunal concluiu pela não proporcionalidade das normas em relação ao art. 10(1) da Lei Fundamental.

**Análise conclusiva crítica**

Sob um aspecto procedimental, a Corte, ao fundamentar juridicamente a sua decisão, adotou uma estrutura decisória robusta e estruturada, na medida em que delimitou com clareza as etapas de julgamento. Em um primeiro momento, delimitou de forma clara o âmbito de proteção do direito à privacidade das telecomunicações. Em seguida, especificou as situações que configuram uma interferência àquele direito fundamental, especificamente quanto à Lei de Telecomunicações e o Código de Processo Penal Alemão. Então, passou a analisar se as interferências identificadas são constitucionalmente justificadas com base no princípio da proporcionalidade.

Ao delimitar o âmbito protetivo, a Corte fez referência a diversos casos por ela mesma julgados, o que indica uma estrutura bem delimitada do direito naquele sistema jurídico. Fora isso, a Corte definiu aspectos relevantes para o caso de modo a contribuir para a clareza da sua decisão. Nesse aspecto, delimitou o conceito do valor que se pretendia proteger através das normas, a segurança pública, considerado como um meio para resguardar interesses protegidos pela lei, suficiente para justificar a interferência aos demais direitos. Ainda, também esclareceu sobre os critérios aplicados para a configuração de um perigo específico, que se baseia na existência de um caso individual, na previsibilidade da ocorrência de danos reais em um certo período de tempo e o fato da causa do perigo poder ser atribuída a pessoas específicas.

Apesar disso, foram identificados alguns aspectos tidos como obscuros, considerando que apesar dos cuidados tomados pela Corte, podem indicar incertezas quanto às diretrizes necessárias para a garantia da segurança dos dados retidos. Alguns direcionamentos são apresentados, como a exigência da legislação prever a notificação posterior à pessoa cujos dados foram utilizados. No entanto, em termos gerais, o elevado padrão de segurança de dados que o Tribunal exige, pouco é especificado. Por exemplo, a Corte se resume a afirmar sobre a necessidade da

atenção a padrões constitucionais específicos quanto à segurança e uso dos dados, transparência e proteção legal. Consequentemente à vagueza da argumentação, essa postura pode dificultar a implementação prática do monitoramento desses dados.

É certo que há que se discutir se esse seria o papel do Poder Judiciário ou do Poder Legislativo, mas ainda assim uma maior especificação das possibilidades protegidas pela Lei Fundamental quanto a esses aspectos contribuiria para uma maior eficácia decisória. Da mesma forma, a Corte direciona a possibilidade da obtenção de dados retidos, desde que um juiz os autorize. Entretanto, não apresenta com clareza quais direcionamentos podem ser tomados pelo julgador.

Nesse aspecto, ainda há incertezas quanto ao uso dos dados encobertos e dos dados obtidos incidentalmente, na medida em que ficam a critério do decisionismo judicial, a ser analisado caso a caso. Fora isso, outro ponto da decisão que pode gerar incertezas está na linha limítrofe entre os dados retidos serem utilizados de forma direta ou indiretamente. Neste caso, a Corte considerou que os requisitos constitucionais são menos rigorosos, mas deixou de analisar especificamente a respeito do risco potencial que pode ser gerado pela obtenção massiva de dados indiretos, o que pode afetar a privacidade.

Por fim, um dos critérios mencionados para medir o grau de vigilância dos dados a serem obtidos se refere à ocorrência de crimes graves. No entanto, a decisão deixou de especificá-los, o que também pode dificultar a aplicação prática dos contornos apresentados em uma lei futura.

Quadro sinóptico BvR 256/08, 263/08 e 586/08

| |
|---|
| **1 - Qual o pedido feito na ação? Ou seja, quais foram os elementos fáticos e legais? Quem propôs a ação?**<br>O pedido feito nas ações BvR 256, BvR 263 e BvR 586, de 2008, no âmbito do Tribunal Constitucional Federal Alemão (TCFA), versam acerca de reclamações constitucionais contra a retenção de dados de telecomunicações prevista pela Lei de Telecomunicações, pois, de acordo com os reclamantes, tal prática viola os direitos fundamentais previstos na Constituição. Os proponentes das ações permaneceram em anonimato. |
| **2 - Qual a efetiva decisão da Corte? A Corte (STF/TCF) privilegia a segurança pública ou o direito à proteção de dados pessoais?**<br>O Tribunal Constitucional Alemão, após discussões quanto às questões fáticas e jurídicas, decidiu pela declaração de nulidade dos artigos §§ 113a e 113b da Lei de Telecomunicações e do artigo § 100g(1), primeira frase do Código de Processo Penal Alemão. Por conseguinte, suas disposições não seriam mais aplicadas, embora não houvesse propriamente a declaração da inconstitucionalidade. Foi privilegiado, portanto, a proteção dos dados pessoais, em detrimento da segurança pública. |
| **3- As Cortes utilizam o princípio ou critério da proporcionalidade como método de solução dos conflitos entre a liberdade de expressão e os direitos de personalidade na rede?**<br>Sim, aplicaram o princípio da proporcionalidade para a resolução do caso, com base nas etapas da adequação, necessidade e ponderação ou proporcionalidade em sentido estrito. |

Fonte: Quadro elaborado pelos autores

## Referências


ALEMANHA, Tribunal Constitucional Federal da Alemanha. **1BvR 256, 263, 586/08.** 02 de março de 2010.

DIMOULIS, Dimitri; MARTINS, Leonardo. **Teoria Geral dos Direitos Fundamentais**. São Paulo: Revista dos Tribunais, 2022.

FARIAS, E. **Liberdade de expressão e comunicação: teoria e proteção constitucional.** São Paulo: Revista dos Tribunais, 2004.

ORWELL, George. **"1984"**. 38º reimpressão. São Paulo: Cia das Letras, 2009.

UNIÃO EUROPEIA. **Diretiva 2006/24/CE do Parlamento Europeu e do Conselho, de 15 de março de 2006, relativa à conservação de dados gerados ou tratados no âmbito da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações e que altera a Diretiva 2002/58/CE.** Jornal Oficial da União Europeia, L 105, 13 de abril de 2006. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32006L0024.

# Conclusão

Carlo José Napolitano

Como o próprio título deste e-book indica, a ideia inicial era apontar os pontos de convergências e divergências nos Tribunais Constitucionais brasileiro e alemão quando da análise e do julgamento de casos relacionados à proteção de dados/ compartilhemento de dados, privacidade e direito à informação.

Após a apresentação e análise dos 13 casos selecionados na pesquisa, é possível apontar algumas sínteses conclusivas, levando em consideração, especialmente as perguntas norteadoras da pesquisa, mesmo que essas sínteses sejam preliminares, considerando que o projeto ainda está em andamento, com previsão de término para março de 2025.

É importante pontuar que dos 13 casos aqui apresentados, 10 deles foram julgados pelos tribunais investigados, e 3, ainda estão pendentes de julgamento pelo STF.

Em relação à primeira pergunta norteadora, em especial, a identificação de quem propôs a ação, é possível verificar que os demandantes podem ser, em regra, agrupados em grupos de interesse: partidos políticos (2 casos); Conselho Federal da Ordem dos Advogados do Brasil (2 casos); empresas (3 casos) e Ministério Público (1), ou seja, os interesses envolvidos são diversos, dos interesses coletivos/gerais, aos particulares e empresariais. Não foi possível identificar os autores nos processos do TCFA por estarem anonimizados.

Em relação à segunda pergunta norteadora, se o tribunal privilegia os direitos de personalidade ou o direito à informação, houve um privilégio em relação à privacidade/personalidade no TCFA, enquanto no STF o direito preferencial foi o acesso à informação.

Nos quatro casos analisados por Enrico e Samara, verifica-se que em todos eles o TCFA privilegiou o direito de personalidade. A mesma conclusão foi extraída no caso do TCFA analisado por Laura, Luiz e Sarah. Verifica-se que o tribunal alemão, nos cinco casos aqui analisados, privilegiou os direitos da personalidade.

Nos casos do STF analisados por Regis e Samara verifica-se que o Supremo permite o compartilhamento de dados, desde que observados alguns parâmetros. Nos 4 casos analisados pode se inferir que em 3 deles houve um privilégio ao compartilhamento de informações.

Os dois casos sobre investigação criminal analisados por Carlo, Deborah, Isadora, Lucas e Tatiana ainda estão pendentes de julgamento, porém é possível apontar que o STF tenderá a privilegiar os direitos de personalidade nesses casos.

No caso sobre divulgação de processos, ainda em julgamento pelo STF, e analisado por Arthur e Renato, é possível indicar que o Supremo tenderá a priorizar o direito à informação.

Em relação ao acesso à banco de dados, caso analisado por Carlo, Deborah, Lucas e Tatiana, verifica-se que o STF privilegiou o acesso aos dados pessoais do contribuinte.

Resumidamente, pode se concluir que o TCFA tende a privilegiar os direitos de personalidade, pelo menos é o que se extrai dos casos aqui analisados, pois dos cinco analisados neste recorte, em todos, houve um privilégio em relação a esses direitos. No caso do STF, dos casos já julgados (cinco), houve prevalência do direito à informação em quatro deles.

Em relação à terceira pergunta norteadora, se os tribunais usam o critério da proporcionalidade para decidir os casos, dos 5 processos do TCFA analisados, em todos, houve a aplicação do critério. Nos cinco casos já decididos pelo STF, em quatro deles, ocorreu a utilização da técnica.

Por fim, é possível concluir, mesmo que de forma preliminar, que os dois tribunais convergem no que diz respeito à utilização do critério da ponderação para a solução dos conflitos, contudo divergem no âmbito de proteção, podendo extrair, mesmo que

provisoriamente, que no TCFA há um caminho preferencial em relação aos direitos de personalidade, enquanto o STF dá preferência ao direito à informação/compartilhamento de dados.

# Autores

**Arthur Almeida de Oliveira**, Bacharel em Jornalismo pela Universidade Estadual Paulista "Júlio de Mesquita Filho" (Unesp). Foi bolsista PIBIC/CNPq e ICTEx/PROPe/AREX/Unesp, tendo realizado estágio de pesquisa na Escola de Direito da Universidade do Minho (Portugal). arthur.a.oliveira@unesp.br

**Carlo José Napolitano**, Departamento de Ciências Humanas, da Faculdade de Arquitetura, Artes, Comunicação e Design, Unesp/Bauru e Programa de Pós-graduação em Comunicação, UNESP/Bauru. carlo.napolitano@unesp.br

**Deborah Cunha Teodoro**, Doutora em Comunicação pela Universidade Estadual Paulista (UNESP) Faculdade de Arquitetura, Artes, Comunicação e Design, Bauru. deborah.teodoro@unesp.br

**Enrico Lentini Gibotti**, Mestrando em Direito pela Pontifícia Universidade Católica de Campinas (PUC-CAMPINAS), ligado à linha de pesquisa de Direitos Humanos e Cooperação Internacional. enricolen@hotmail.com

**Isadora Pinto de Sousa**, graduanda em jornalismo pela Faculdade de Arquitetura, Artes, Comunicação e Design, Bauru. Bolsista de Iniciação Científica neste projeto financiado pelo CNPq. isadora.p.sousa@unesp.br

**Lucas Catib de Laurentiis**, Faculdade de Direito da Pontifícia Universidade Católica de Campinas e Programa de Pós-Graduação Direito/PucCamp. lucas.laurentiis@gmail.com

**Luiz Henrique Ranzani**, Mestre em Comunicação (Processo FAPESP nº 2023/03087-1) pela Universidade Estadual Paulista (UNESP) Faculdade de Arquitetura, Artes, Comunicação e Design, Bauru. luiz.ranzani@unesp.br

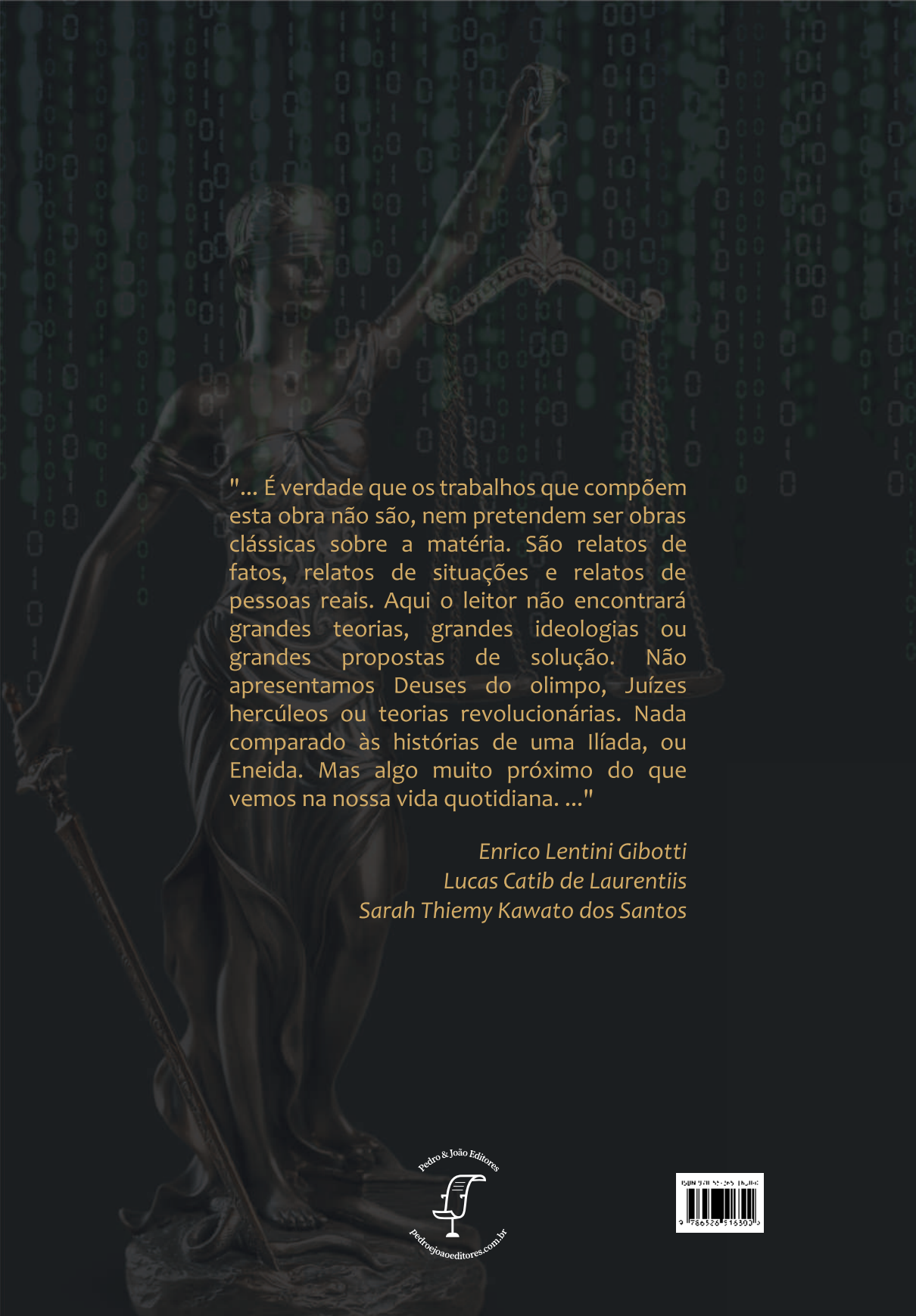
**Régis Martins**, Advogado, especialista em Direito Público, mestre em Ciência da Informação pela Faculdade de Filosofia e Ciências da Universidade Estadual Paulista "Júlio de Mesquita Filho" - Câmpus de Marília e doutorando pela Faculdade de Arquitetura, Artes, Comunicação e Design da Universidade Estadual Paulista "Júlio de Mesquita Filho" - Câmpus de Bauru.

**Renato Sobhie Zambonatto**, Bacharel em Direito pelo Centro Universitário de Bauru (ITE-Bauru). Pós-graduado em Direito Penal e em Perícia Criminal e Investigação Forense. Mestrando em Comunicação pelo Programa de Pós-graduação em Comunicação da Faculdade de Arquitetura, Artes e Comunicação da Universidade Estadual Paulista (FAAC/Unesp). renato.zambonatto@unesp.br

**Samara Meneses Brito**, aluna do curso de Jornalismo da Faculdade de Arquitetura, Artes, Comunicação e Design, UNESP/Bauru. Bolsista PIBIC/CNPq. samara.meneses@unesp.br

**Sarah Thiemy Kawato dos Santos**, Advogada, mestranda em Direitos Humanos e Desenvolvimento Social pela Pontifícia Universidade Católica de Campinas. E-mail: sarahthiemy.adv@gmail.com

**Tatiana Stroppa**, Centro Universitário de Bauru (ITE-SP), Faculdade Iteana de Botucatu e Programa de Pós-Graduação em Direito (ITE), doutora em Direito pelo Programa de Pós-graduação ITE. tatianastroppa@hotmail.com



"... É verdade que os trabalhos que compõem esta obra não são, nem pretendem ser obras clássicas sobre a matéria. São relatos de fatos, relatos de situações e relatos de pessoas reais. Aqui o leitor não encontrará grandes teorias, grandes ideologias ou grandes propostas de solução. Não apresentamos Deuses do olimpo, Juízes hercúleos ou teorias revolucionárias. Nada comparado às histórias de uma Ilíada, ou Eneida. Mas algo muito próximo do que vemos na nossa vida quotidiana. ..."

*Enrico Lentini Gibotti*
*Lucas Catib de Laurentiis*
*Sarah Thiemy Kawato dos Santos*

Pedro & João Editores
pedroejoaoeditores.com.br