TJPR

TRIBUNAL DE JUSTIÇA
DO ESTADO DO PARANÁ

# REVISTA DA OUVIDORIA

Edição *2020*

**GESTÃO 2019-2020**

**Presidente**

Des. Adalberto Jorge Xisto Pereira

**Ouvidora-Geral**

Desª. Ana Lúcia Lourenço

**Ouvidora**

Desª. Maria Aparecida Blanco de Lima

**Juízes Auxiliares**

Dra. Fabiane Pieruccini

Dr. Francisco Cardozo Oliveira

**Supervisora**

Roseliz Patitucci

**Equipe de Apoio**

Bianca Buck Perina

Guilherme de Macedo Malheiros

Luciana Caroline Dias Reisdorfer

Mara Rúbia Santana da Cruz

Scheilla de Lara Marçal

**Estagiários**

Carlos de Paula Soares Filho (estagiário de pós-graduação)..

Gabriela Natássia Godoi Marques (estagiário de pós-graduação).

Sheyla do Nascimento Teixeira (estagiária de graduação)

**Convidados – Artigos**

Desª Joeci Machado Camargo e Dr. Rafael Corrêa

Dr.Gabriel Schulman e Dr. Lucas Schirru

Desª Ana Lúcia Lourenço e Mestre João Daniel Vilas Boas Taques

**Texto, Pesquisas e Gráficos**

Ana Lúcia Lourenço, Francisco Cardozo Oliveira,Roseliz Patitucci, Scheilla de Lara Marçal, Carlos de Paula Soares Filho e Gabriela Natássia Godoi Marques

**Revisão**

Francisco Cardozo Oliveira

2ª edição – 2020

Ouvidoria-Geral da Justiça

www.tjpr.jus.br/ouvidoria

# ÍNDICE

# APRESENTAÇÃO

A Lei 13.709/18 dispõe sobre o tratamento de dados pessoais, nos meios físicos e digitais, inclusive por pessoa jurídica de direito público, com o objetivo de proteger os direitos fundamentais da liberdade e de privacidade e o livre desenvolvimento da personalidade. As normas gerais contidas na Lei são de interesse nacional e devem ser observadas pela União, Estados, Distrito Federal e Municípios.

No âmbito da Lei Geral de Proteção de Dados, também conhecida como LGPD, o tratamento dos dados pessoais pode ser realizado por dois agentes de tratamento, o controlador e o operador. O controlador é definido pela Lei como a pessoa natural ou jurídica, de direito público ou privado, a quem compete tomar as decisões referentes ao tratamento de dados pessoais. Na Administração Pública, o controlador será a pessoa jurídica do órgão ou entidade pública sujeita à Lei, representada pela autoridade imbuída de adotar as decisões acerca do tratamento de tais dados.

O operador é a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador, aí incluídos agentes públicos no sentido amplo que exerçam tal função, bem como pessoas jurídicas diversas daquela representada pelo controlador, que exerçam atividade de tratamento no âmbito de contrato ou instrumento congênere.

A Lei nº 13.853/2018, veio trazer algumas alterações à lei 13.709/18 para além de dispor sobre a proteção de dados pessoais, criar a Autoridade Nacional de Proteção de Dados (ANPD), que é responsável pela fiscalização e pela regulação da LGPD, vinculada à Presidência da República. A estrutura regimental da ANPD foi aprovada pelo Decreto nº 10.474 de 26 de agosto de 2020.

A lei prevê também a figura do encarregado, que é a pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a já mencionada Autoridade Nacional de Proteção de Dados (ANPD).

Considera-se "tratamento de dados" qualquer atividade que utilize um dado pessoal na execução da sua operação, como, por exemplo: coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

A Recomendação nº 73/20 do Conselho Nacional de Justiça (CNJ) orienta a adequação dos órgãos do Poder Judiciário à Lei Geral de Proteção de Dados. Entre as recomendações, destaca-se a criação de grupos de trabalho para estudo e identificação das medidas necessárias à implementação da LGPD, a partir das quais o CNJ formulará a política nacional para os tribunais e conselhos de Justiça, englobando questões como organização e comunicação, direitos do titular, gestão de consentimento, retenção de dados e cópia de segurança, contratos e plano de respostas a incidentes de segurança com dados pessoais.

A edição 2020 da Revista Ouvidoria - TJPR reuniu informações acerca das interpretações sobre o tema proteção de dados pessoais. Destaca-se o papel da jurisprudência dos tribunais na aplicação ao direito de proteção a estes dados, assim como o trabalho da Ouvidoria do Tribunal de Justiça do Paraná no atendimento de manifestações relacionadas ao exercício do direito proteção de dados.

A Revista da Ouvidoria - TJPR, edição no1 - 2020, está dividida em quatro seções.

A primeira seção está destinada aos artigos de juristas e profissionais do direito. A Desembargadora do TJPR Joeci Camargo e o Assessor Jurídico Rafael Corrêa escrevem sobre "**A tutela da privacidade das relações familiares: entre a responsabilidade parental e as disposições da Lei Geral de Proteção de Dados**"; os Professores Doutores Gabriel Schulman e Lucas Schirru tratam do tema: "**Pequenos titulares e grandes desafios, a proteção de dados pessoais de crianças e adolescentes: um debate sobre melhor interesse, (des)equilíbrios, e lgpd a partir do episódio "*arkangel*" da série** *black mirror*", e ainda por último a contribuição desta subscritora juntamente com o bacharel João Daniel Vilas Boas Taques, que foi estagiário de pós-graduação na Ouvidoria de Justiça, abordando o **"Papel das Ouvidorias Públicas na implementação da Lei Geral de Proteção de Dados (LGPD)".**

Na segunda seção elabora-se uma análise acerca do conteúdo da jurisprudência do **Tribunal de Justiça do Paraná** a respeito da proteção de dados pessoais.

A terceira seção se dedica a organizar a jurisprudência do **STF, STJ e TRF4**, acerca de casos envolvendo também a proteção de dados com comentários e remissão a links para aprofundamento da pesquisa pelo leitor e usuário.

Na quarta parte é feita análise dos pedidos de manifestações e o modo como a **Ouvidoria do Tribunal de Justiça do Paraná** desenvolve o procedimento de proteção de dados tomando como parâmetro legal de regulação a Lei de Acesso à Informação (LAI) e observando as premissas aceitas antes da entrada em vigor da Lei de Proteção de Dados no Brasil (LGPD).

Espera-se que o material informativo reunido nesta edição 2020 da Revista da Ouvidoria - TJPR sirva ao propósito de suscitar o interesse do cidadão pelo exercício e efetividade do direito a proteção dos dados pessoais dos indivíduos, necessário a construção do Estado Democrático de Direito.

Agradeço o empenho de toda a minha equipe de servidores da Ouvidoria e principalmente ao Dr. Francisco Cardozo Oliveira, MM. Juiz de Direito Substituto de Segundo Grau junto à 4ª Câmara Cível e Juiz Auxiliar na Ouvidoria de Justiça deste Tribunal, o verdadeiro idealizador desta e da primeira edição.

**Desembargadora Ana Lúcia Lourenço**

*Ouvidora-Geral do Tribunal de Justiça do Paraná*

# ARTIGOS



# A tutela da privacidade das relações familiares: entre a responsabilidade parental e as disposições da Lei Geral de Proteção de Dados

*Joeci Machado Camargo*[1]

*Rafael Corrêa*[2]

**Resumo:** *O presente trabalho tem como objetivo ponderar a proteção da privacidade e dados pessoais no âmbito das relações estabelecidas nos núcleos familiares, tendo em conta não apenas as normativas estabelecidas pela Lei Geral de Proteção de Dados, mas também ante a indestacável responsabilidade que deve marcar o exercício da autoridade parental no cuidado com crianças e adolescentes, em consonância com o viés de autonomia existencial que atualmente marca a ordem jurídica brasileira.*

**Palavras-chave:** *dados pessoais – privacidade – família – criança – adolescente.*

## Breve Introdução

A *Lei Geral de Proteção de Dados Pessoais* (LGPD), estruturada por meio da Lei nº 13.709/2018, consolida avanço inquestionável na tutela da privacidade neste momento em que a sociedade brasileira – e o mundo, como um todo – encontra-se conectada por meio do uso incessante de plataformas digitais. Não é exagero crer ou afirmar que parcela majoritária dos nossos atos cotidianos se dá por meio de interações em redes sociais, aplicativos de compras e sistemas de envio e recebimento de mensagens, mecanismos cujo uso restou amplamente potencializado após a expansão pandêmica da *COVID-19*.

Esse cenário, de todo contemporâneo à realidade brasileira, coloca a privacidade e os dados pessoais como protagonistas da atenção destinadas por gigantes como *Google*,

1 Desembargadora do Tribunal de Justiça do Estado do Paraná. Idealizadora e Coordenadora do Programa Justiça no Bairro (TJPR). Integrante do Conselho da Magistratura do Tribunal de Justiça do Estado do Paraná. Vencedora de Prêmio pelo *World Family Summit* realizado pela Organização das Nações Unidas – ONU.

2 Mestre em Direito das Relações Sociais pela Universidade Federal do Paraná. Especialista em Direito Público pela Escola da Magistratura Federal do Paraná. Professor de Direito Civil, Direito do Consumidor e Direito Constitucional do Centro Universitário Opet (UniOpet). Assessor Jurídico no Tribunal de Justiça do Estado do Paraná.

*Amazon, Facebook, WhatsApp* e *Microsoft* – isso para firmarmos apenas alguns exemplos de plataformas digitais que, de um modo ou de outro, ocupam boa parte dos atos de consumo na atual quadra da história de nossas vidas. Bem por isso é que se assume o fato de que as relações sociais e econômicas (principalmente estas) se dão impulsionadas pela coleta e processamento de dados pessoais, informações sensíveis sobre todas as pessoas que, com o respectivo tratamento, constituem-se em ativos financeiros de ímpar relevância: ao lado dos lucros urbanos e distribuição de renda, alça-se também a chamada "economia movida a dados".[3]

As preocupações, como se pode presumir, ostentam diversas ordens, mas uma delas em particular chama a atenção desta breve reflexão: de que modo essa nova realidade digital de coleta de dados pode atingir a privacidade do núcleo familiar, principalmente no que toca às crianças e adolescentes, e quais são as ferramentas de proteção contempladas pela LGPD nesse cenário?

Essa preocupação (que assume a roupagem do problema a ser enfrentado neste brevíssimo estudo) decorre, em primeiro lugar, do uso cada vez mais amplo das plataformas digitais por crianças em adolescentes. Em pesquisa realizada no biênio de 2018/2019 pelo *Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação* – **Cetic.br***4*, apontou 86% de crianças e adolescentes de 9 a 17 anos fazem uso constante da internet, do mesmo que 53% deste público-alvo usaram o celular como único dispositivo para uso da internet e 40% usaram conjuntamente celular e computador. Ainda acerca deste mesmo grupo de crianças e adolescentes, 83% fizeram uso de *apps* e transformaram-se em audiência de seriados, filmes e outras mídias visuais estruturadas em plataformas de *streaming*. No que toca ao uso de redes sociais e criação de

3 A referência deriva do termo *data-driven economy*, que reconhece que o maior impulso dado às relações econômicas hoje advém da coleta e processamento de dados, considerados, então, como seu principal insumo. Por todos, ver: FRAZÃO, Ana. Plataformas digitais, *big data* e riscos para os direitos da personalidade. *In*: TEPEDINO, Gustavo; MENEZES, Joyceane Bezerra de [Coord.]. **Autonomia Privada, Liberdade Existencial e Direitos Fundamentais**. Belo Horizonte: Fórum, 2019.

4 COMITÊ GESTOR DA INTERNET NO BRASIL. **Pesquisa Sobre o Uso da Internet por Crianças e Adolescentes no Brasil.** TIC Kids Online Brasil. São Paulo, 2019. Disponível em: < **https://cetic.br/media/docs/publicacoes/216370220191105/tic_kids_online_2018_livro_eletronico.pdf**>. Acesso em julho de 2020.



perfis, 58% das crianças de 9 a 10 anos e 70% de 11 a 12 anos possuem perfis próprios em plataformas como *Facebook* e *Instagram*, dimensão que, para adolescentes de 13 e 14 anos alcança a proporção de 88% e para adolescentes de 15 a 17 anos, 97%.[5]

Em segundo lugar, é importante que não se perca de vista que o núcleo familiar contempla o estabelecimento das relações mais sensíveis e íntimas atreladas a um mesmo grupo afetivo, onde escolhas existenciais são realizadas, planos são traçados e desejos são alcançados. A justificativa para que o referido problema seja então enfrentado reside justamente na possibilidade não só de atingimento e vulneração de tais relações, mas também o seu possível direcionamento, na medida em que as plataformas digitais já citadas, por meio da coleta dos dados fornecidos por pais e filhos para a criação de perfis em redes sociais, escolhas de filmes em *streaming* e cadastro em *sites* de compras, podem direcionar por meio de "sugestões" novos atos de consumo aos seus clientes.[6]

A hipótese de solução ao presente desafio pode residir justamente na identificação de mecanismos concretos derivados da LGPD que outorguem plena autonomia aos titulares dos dados pessoais e aos responsáveis pelo núcleo familiar (vale dizer, pais responsáveis pelos atos de seus filhos), sem, no entanto, colocá-los em dimensão exclusivamente paternalista, próxima a uma imagem de vitimização. Como bem observou Tzevetan Todorov na obra *"O Homem Desenraizado"7*, há um sentimento incessante na sociedade contemporânea para que as pessoas passem a ocupar um papel de passividade próxima à vitimização, onde há sempre alguém a quem atribuir a culpa pelos incessantes revezes da vida.

5 A pesquisa também pode ser encontrada no seguinte trabalho acadêmico: SANCHES, Patrícia Correa; LAMOSA, Elisabeth. **O Direito à Privacidade dos Dados na Seara do Direito das Famílias.** Artigos do Instituto Brasileiro de Direito de Família – IBDFAM. Disponível em: < **https://www.ibdfam.org.br/artigos/1375/O+Direito+%C3%A0+Privacidade+dos+Dados+na+Seara+do+Direito+das+Fam%C3%A-Dlias**>. Acesso em julho de 2020.

6 Em recente entrevista ao canal internacional de notícias BBC, Martin Hilbert (pesquisador dos efeitos do Big Data e professor da Universidade da Califórnia), afirmou que os algoritmos utilizados pelo Facebook podem, por meio de 150 (cento e cinquenta) curtidas, alcançar a compreensão sobre personalidade de uma pessoa de modo mais preciso do que sua própria esposa ou companheira. Isso se dá porque os algoritmos filtram e processam essas informações e as transformam em padrões de comportamento, ativo valiosíssimo para empresas em busca de novos consumidores. LISSARDY, Gerardo. **'Despreparada para a era digital, a democracia está sendo destruída', afirma guru do 'big data'**. Disponível em < **https://www.bbc.com/portuguese/geral-39535650**>. Acesso em agosto de 2020.

7 TODOROV, Tzvetan. **O Homem Desenraizado.** São Paulo: Record, 1999.

Não se trata, portanto, de buscar na LGPD ferramentas que reforcem essa imagem de passividade, mas sim instrumentos que possam reconhecer nos integrantes do núcleo familiar os protagonistas de suas próprias vidas, questão de extrema importância em um momento da história no qual, como já dito, boa parte dos lucros deriva da circulação de dados pessoais.

Sendo assim, a partir do problema, justificativa e hipótese acima apresentados, cumpre destacar que o presente trabalho, dentro de seus breves limites, será pautado em três partes. Na primeira delas, será realizada uma concisa reflexão sobre o atual panorama da privacidade, para que bem se assente este novo "paradigma" das relações sociais e econômicas movidas a dados. Na segunda parte, se cuidará de compreender os possíveis impactos deste novo "paradigma" nas relações familiares, principalmente no que toca aos dados pessoais de crianças e adolescentes, cerne do problema aqui enfrentado. Por derradeiro, na terceira parte será realizada uma breve ponderação sobre os mecanismos constantes na LGPD acerca da proteção necessária e garantia da autonomia pessoal dos integrantes do núcleo familiar, ponderação essa sucedida por uma concisa reflexão apta a rematar as reflexões aqui postas.

Estabelecido o itinerário, passa-se a percorrê-lo.

## Privacidade, autodeterminação informativa e dados pessoais: compreendendo as relações sociais e econômicas movidas a dados

Reconhece-se atualmente a existência do predomínio das grandes plataformas digitais, tais como *Google, Apple, Facebook, Amazon, Microsoft*, dentre outras, que hoje constituem-se como agentes econômicos que operacionalizam grandes empreendimentos a partir de dados pessoais coletados e também disponibilizados pelos seus respectivos usuários.

A partir disso é que surge, nas palavras de Ana Frazão, "a ideia de uma economia movida a dados [...], já que os dados pessoais são hoje o novo 'petróleo' ou principal insumo das atividades econômicas"[8], perspectiva que globalmente vem sendo denominada

8 FRAZÃO, Ana. Plataformas digitais, *big data* e riscos para os direitos da personalidade. *In*: TEPEDINO, Gustavo; MENEZES, Joyceane Bezerra de [Coord.]. **Autonomia Privada, Liberdade Existencial e Direitos Fundamentais**. Belo Horizonte: Fórum, 2019. p. 333.



como *data-driven economy*.[9] Em perspectiva similar, Shoshana Zuboff, professora da *Harvard Business School,* afirma que esse predomínio das plataformas digitais implica na consolidação da "era do capitalismo de vigilância" (*"The Age of Surveillance Capitalism"*), que caracteriza *"uma nova ordem econômica que reivindica a experiência humana como material livre para práticas comerciais ocultas de extração, previsão e venda"10*.

Tal modelo compreende a estruturação das plataformas digitais para além de simples ferramentas de usuários, porquanto, ao erigirem-se como verdadeiro modelo de negócios, criam um ecossistema de interação entre agentes empreendedores que viabiliza substanciais trocas econômicas[11]. Essas trocas, ao seu turno, consubstanciam-se por meio da coleta de dados pessoais dos usuários e da utilização de produtos dotados de interfaces tecnológicas que os conectam com a internet e a outros dispositivos. É nesse espaço de inovação que Eduardo Magrani define a consolidação da "Internet das Coisas", globalmente referida pela sigla *IoT* (*Internet of Things*), concentrada em "[...] objetos que interagem uns com os outros e processam dados em um contexto de hiperconectividade"[12].

Esse fenômeno deve ser encarado com cautela, isso porque a expansão dos algoritmos (ferramenta essencial da *Big Data, Data Science* e *IoT*) implica também em outros riscos: por meio da sistemática de *machine learning* e *deep learning*, os algoritmos também podem "aprender" por meio da interação com os usuários e modificar a sua estrutura, adquirindo, como alerta Ana Frazão, "[...] o poder de decodificar as pegadas digitais das pessoas, inferindo e predizendo até mesmo aquilo que ninguém revela e que muitas vezes não tem nem mesmo consciência"[13].

9 WAHLSTER, Wolfgang *et al* [Editors]. **New Horizons for a Data-Driven Economy**. Roadmap for usage and exploitation of Big Data in Europe. Springer International Publishing, 2016 [livro eletrônico].

10 ZUBOFF, Shoshana. **The Age of Surveillance Capitalism**. The fight for a human future at the new frontier of power. New York: Public Affairs, 2019 [livro eletrônico]. Já na abertura da obra, Zuboff assim consigna o primeiro verbete definidor do "capitalismo de vigilância": "1. A new economic order that claims human experience as free raw material for hidden comercial practices of extraction, predictions, and sales." Posição 102.

11 FRAZÃO, Ana.Op. *Cit*.. p. 334.

12 MAGRANI, Eduardo. **A Internet das Coisas.** Rio de Janeiro: FGV Editora, 2018 [livro eletrônico].

13 FRAZÃO, Ana. Plataformas digitais, *big data* e riscos para os direitos da personalidade. *In*: TEPEDINO, Gustavo; MENEZES, Joyceane Bezerra de [Coord.]. **Autonomia Privada, Liberdade Existencial e Direitos Fundamentais**. Belo Horizonte: Fórum, 2019. p. 340.

A partir disso, também é possível perceber que as tecnologias de coleta e processamento de dados pessoais passaram a abrir espaço para a comercialização de outros espaços de nossas vidas, até então ainda não explorados. Essa é a preocupação desenhada por Tim Wu, professor da *Columbia Law School* e precursor da chamada "teoria da economia da atenção" (*attention merchants*).

Segundo Wu, a mercantilização da atenção representa fração majoritária da economia atual, sendo o direcionamento de nossa atenção cada vez mais reconhecido como uma *commodity*, fenômeno que estabelece um modelo de negócios que influencia nossas escolhas, podendo mudar e modelar radicalmente a forma pela qual vivemos. Assim, ao reconhecer a grande parcela de tempo em que permanecemos "distraídos" rolando telas de redes sociais, afirma Wu que "[...] o que está em jogo é natureza de nossas próprias vidas. Porque como gastamos o recurso brutalmente limitado de nossa atenção poderá determinar essas vidas em um nível que muitos talvez prefiram não pensar sobre isso".[14]

Todos esses fatores expressam a estruturação desta "economia movida a dados" que ressignifica nossas relações interpessoais tanto no âmbito mais íntimo de nossa existência quanto nas relações de consumo e de matiz econômico que entabulamos em nossa existência correlacional em sociedade – isso, a rigor, sem uma regulação adequada da ordem jurídica.

O que se evidencia, conforme aponta Eduardo Magrani, ante a ausência de regulação adequada pelo Direito sobre esse cenário, é uma "[...] autorregulação do próprio mercado e uma regulação realizada muitas vezes através do *design* dessas novas tecnologias", fenômeno que o autor denomina de tecnorregulação; e acrescenta: "A tecnologia está avançando mais rápido do que nossa habilidade de garantir a tutela dos direitos individuais e coletivos"[15].

14 WU, Tim. **The Attention Merchants.** The epic struggle to get inside our heads. London: Atlantic Books Ltda, 2017 [livro eletrônico]. O conteúdo acima resulta da tradução livre do seguinte trecho: "Ultimately, it is no tour nation or culture but the very nature of our lives that is at stake. For how we spend the brutally limited resource of our attention will determine those lives to a degree most of us may prefer not to think about."

15 MAGRANI, Eduardo. **Entre Dados e Robôs**. Ética e privacidade na era da hiperconectividade. Série Pautas em Direito. Porto Alegre: Arquipélago Editorial, 2019 [livro eletrônico].



Esse *delay* do Direito em face do avanço tecnológico exige uma análise mais verticalizada e precisa acerca do elemento essencial ao desenvolvimento da personalidade humana que vem sendo manejado pelas plataformas que esteiam a *data-driven economy*: este elemento é a privacidade, permeada por aquilo que hoje se entende por dados pessoais, partindo-se da noção de autodeterminação informativa[16] estabelecida por Stefano Rodotà.[17]

Mostra-se crucial, portanto, que seja assegurado a cada pessoa o controle sobre suas próprias informações, sobre seus dados pessoais – daí a efetiva compreensão de que tal fenômeno também coloca em marcha uma mudança na dimensão do próprio conceito de privacidade, que deixa de estar atrelado à antiga concepção do "direito de estar só" para alcançar o referido significado de autodeterminação informativa.[18]

## O Impacto da Expansão das Plataformas Digitais e Coleta de Dados Pessoais nos Núcleos Familiares

Todos esses fatores contribuem sobremaneira para modificar a forma pela qual as relações interpessoais são travadas em diversos níveis – e a ambiência familiar não resta excluída desses impactos.

Não se trata apenas de reconhecer que, conforme se apontou acima a partir das teorizações atreladas à chamada "economia da atenção", potenciais escolhas existenciais

16 O paradigma da autodeterminação informativa, que envelopa a dimensão decisional das pessoas sobre suas informações e dados, é adotada pela doutrina civilista de escol no Brasil. Nesse sentido, ver: JÚNIOR, Marcos Ehardt *et al*. Breves notas sobre a ressignificação da privacidade. *In*: **Revista Brasileira de Direito Civil – RBDCivil**. Belo Horizonte. Vol. 16. Abr/Jun 2018. p. 35.56; SHCREIBER, Anderson. Direito à privacidade no Brasil: avanços e retrocessos em 25 anos de Constituição. *In*: CLÈVE, Clémerson Merlin. **Direitos Fundamentais e Jurisdição Constitucional.** São Paulo: Editora Revista dos Tribunais, 2014. p. 183-201.

17 RODOTÀ, Stefano. **A Vida na Sociedade de Vigilância**. A privacidade hoje. Rio de Janeiro: Renovar, 2008. p. 92. Segundo o autor: "[...] a privacidade pode ser definida, mais precisamente, em uma primeira aproximação, como do direito de manter o controle sobre as próprias informações. [...] Trata-se, em especial, de informações relacionadas às opiniões políticas e sindicais, além daquelas relativas à raça ou credo religioso."

18 Neste sentido, ver: CORRÊA, Rafael. Os Plúrimos Sentidos Da Privacidade E Sua Tutela: A questão da proteção de dados pessoais e sua violação na atual construção jurisprudencial brasileira. *In*: **ANIMA**. Revista Eletrônica do Curso de Direito das Faculdades Opet, v. IX, p. 1-19, 2017. Disponível em: < http://www.anima-opet.com.br/pdf/anima16/1.Os-Plurimos-Sentidos-da-Privacidade-e-sua-Tutela-Rafael-Correa.pdf>. Acesso em agosto de 2020.

nas relações familiares seja influenciadas pelo alcance das plataformas digitais, mas de constatar que boa parte das crianças e adolescentes no Brasil, ao menos a partir de 2016, estruturam parcela significativa de suas informações, escolhas e opções pessoais por meio de plataformas digitais.

Em pesquisa realizada pelo *Instituto Play* (2016), restou apontado que crianças e adolescentes utilizam plataformas digitais para acessar e descobrir novidades, bem como para se informar de modo geral, tanto que 61% do público consultado afirmou fazer uso do *YouTube* ou *Facebook* para tal finalidade.[19]

Todo esse uso, em maior ou menor medida, dá-se de modo autônomo pelas crianças e adolescentes. De acordo com a pesquisa envidada pelo *Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação – cetic.br*, mencionada na introdução deste estudo, 70% dos pais acreditam que seus filhos fazem uso de aplicativos e plataformas digitais de modo efetiva e integralmente seguro, alijados de quaisquer riscos; entretanto, 50% das crianças e adolescentes consultadas afirmaram que, em contrapartida, todas as atividades realizadas por elas *on line* não são de conhecimento de seus pais, sendo boa parte delas efetivadas sem autorização ou mesmo supervisão já que, para tanto, pasta que utilizem seus próprios dados pessoais independente do controle de seus responsáveis.[20]

Esses apontamentos podem revelar um dado bastante complexo, isso porque o uso constante e incessante de plataformas digitais pode contribuir na formação de crianças e adolescentes na mesma medida em proporção que pode atingir aspectos importantes de seu relacionamento interpessoal.

Não se pode perder de vista que, conforme bem explica Ricardo Calderón, compreender a família como espaço de realização aberta de seus integrantes é medida não apenas consoante à ordem constitucional em vigor mas também como elemento indestacável

19 INSTITUTO PLAY. (2016). **Prazer: Somos a Geração alpha**. Gente, uma conexão Globosat. Acesso em 27 de junho de 2019, disponível em: <http://gente.globosat.com.br/wp-content/uploads/2018/06/Globosat-Gente-Geracao-Alpha.pdf>. Acesso em agosto de 2020.

20 COMITÊ GESTOR DA INTERNET NO BRASIL. **Pesquisa Sobre o Uso da Internet por Crianças e Adolescentes no Brasil.** TIC Kids Online Brasil. São Paulo, 2019. Disponível em: < https://cetic.br/media/docs/publicacoes/216370220191105/tic_kids_online_2018_livro_eletronico.pdf>. Acesso em julho de 2020.



para tê-la como "[...] o espaço para o livre desenvolvimento da personalidade individual", reconhecendo-se, sem prejuízo disso, que os "[...] paradigmas sociais vigentes refletem na forma de convivência".[21] Logo, mesmo que se tenha essa coerente concepção de família, não se pode ignorar que fatores externos podem moldar a estruturação das relações travadas no núcleo familiar – influência essa que, como apontado no tópico anterior, pode trazer severos prejuízos.

A esses fatores somam-se também as circunstâncias nas quais se estabelecem as premissas para o uso de redes sociais entre crianças e adolescentes, premissas essas que correspondem a uma superexposição e crescente interesse na obtenção "curtidas" a cada postagem e a cada interação.

Sobre este aspecto, aponta Marcelo Romão Marineli a estruturação de dois tipos de ameaças: a primeira, considerada como horizontal, decorre dos próprios usuários de determinadas plataformas e aplicativos, que violam direitos alheios por meio de indicação não consentida de fatos e imagens; e a segunda, considerada como vertical, onde as plataformas sociais, pela sua "sofisticação", otimizam o tratamento dos dados pessoais disponibilizados e expõem hábitos e preferências de jovens e adultos para empresas interessadas em estabelecer padrões de consumo.[22]

Outro efeito pernicioso que deriva do uso excessivo das redes sociais e plataformas digitais, correspondente à ameaça horizontal acima indicada, é o chamado *cyberbullying*, prática de intimidação e ofensas consolidadas por meio de postagens e compartilhamentos de arquivos. Como exemplo, cite-se o caso de uma adolescente de 16 anos de idade que teve fotos íntimas divulgadas por um amigo da mesma idade e também usuário de redes sociais[23], fato que lhe abalou severamente e a conduziu à prática de suicídio.

21 CALDERÓN, Ricardo Lucas. **Princípio da Afetividade no Direito de Família.** Rio de Janeiro: Renovar, 2013. p. 35.

22 MARINELI, Marcelo Romão. **Privacidade e Redes Sociais Virtuais.** Sob a égide da 12.965/2014 – Marco Civil da Internet e da Lei 13.709/2019 – Lei Geral de Proteção de Dados Pessoais [livro eletrônico]. São Paulo: Thomson Reuters Brasil, 2019.

23 **Adolescente é encontrada morta após ter sua foto seminua publicada na Internet.** JCNET. 2013. Disponível em: <https://m.jcnet.com.br/Nacional/2013/11/adolecente-e-encontrada-morta-apos-ter-sua-foto-seminua-publicada-na-internet.html>. Acesso em agosto de 2020.

Diante desse cenário, urge perquirir qual o instrumental ofertado pela LGPD à proteção e tratamento de dados pessoais em âmbito familiar, principalmente no que toca às crianças e adolescentes.

## O Papel da LGPD na Tutela e Tratamento de Dados Pessoais de Crianças e Adolescentes

Uma das premissas essenciais estabelecida na *Lei Geral de Proteção de Dados* brasileira é a proteção da privacidade associada à autodeterminação informativa e ao livre desenvolvimento da personalidade, conforme se depreende de seu art. 2º, incisos I, II e VII. Isso implica em reconhecer uma especial atenção à autonomia dos titulares dos dados pessoais, que poderão, tendo em conta a concepção renovada de privacidade antes mencionada, melhor controlar (ao menos em sede de pressuposto) as suas próprias informações em ambiência digital.

Como anotado por Rony Vainzof, a premissa acima aludida vai além da tutela da esfera íntima da pessoa, "[...] pois atinge também emanações notoriamente de natureza pública dos titulares, [...] incluindo o tratamento de dados pessoais cujo acesso é público, que deverá considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização"[24].

Do mesmo modo, o art. 6º, inciso IV da LGPD estabelece como um dos princípios cardeais ao tratamento dos dados coletados o livre acesso aos respectivos titulares, garantindo a eles o acesso facilitado e também gratuito sobre todos os detalhes acerca do tratamento realizado, seja sobre sua finalidade, seja sobre seu método procedimental.

Há que se destacar, do mesmo modo, a especificação dada pela legislação em tela ao tratamento a ser destinado aos chamados *dados pessoais sensíveis*, que congrega os traços de informações que traduzem de modo mais preciso e contundente os contornos da personalidade de cada pessoa, englobando escolhas pessoais, políticas ou mesmo ideológicas.[25]

24 VAINZOF, Rony. Art. 2º *In*: OPICE BLUM, Renato; MALDONADO, Viviane Nóbrega [Coords.]. **LGPD – Lei Geral de Proteção de Dados Comentada.** 2ª Ed [livro eletrônico]. São Paulo: Thomson Reuters, 2019.

25 Sobre o tema, por todos, ver: DONEDA, Danilo. **Da Privacidade à Proteção de Dados Pessoais**. Rio de Janeiro: Renovar, 2006.



Neste aspecto, as disposições dos arts. 5º, 11, 12 e 13 da *Lei Geral de Proteção de Dados* brasileira exige o consentimento expresso do titular para a realização do referido tratamento, tornando ainda mais excepcional a sua realização sem a autorização expressa na medida em que resta atrelada a finalidades que, em maior ou menor passo, correspondem a determinações judiciais e interesses de ordem pública.

Entretanto, nada obstante a amplitude das disposições normativas aludidas acima, no que toca ao interesse das crianças e adolescentes a tutela de dados pessoais e seu respectivo tratamento resta reservado a apenas um dispositivo, o art. 14 e parágrafos da LGPD.

De plano, extrai-se que o art. 14, *caput* da LGPD a premissa valorativa de que o tratamento de dados pessoais de crianças e adolescentes deve atender ao seu melhor interesse, questão essa plasmada em diversas proposições da Lei nº 8.609/1990, que estabeleceu o Estatuto da Criança e do Adolescente.

O diálogo entre a *Lei Geral de Proteção de Dados* com as normas lançadas na legislação de proteção de menores é bastante clara, já que o consentimento para o tratamento de dados contemplado no art. 14 da LGPD parte da distinção que o ECA faz, em seu art. 2º, *caput*, entre crianças (pessoa de até doze anos incompletos) e adolescentes (pessoa de doze anos completos a dezoito anos de idade).

Assim, o art. 14, §1º da LGPD aponta que, no que toca às crianças, o tratamento de dados pessoais depende essencialmente com o consentimento expresso e específico de ao menos um dos pais ou responsáveis. Nada obstante tal previsão, é importante não esquecer, conforme apontado nos tópicos anteriores, que pesquisas recentes apontam que diversas crianças fazem uso de aplicativos e plataformas digitais, por meio da concessão de seus próprios dados, sem a supervisão ou consentimento dos pais.

Aqui, há que se considerar a necessidade de otimização e modificação das plataformas digitais para que a aceitação dos serviços prestados dependa de um conjunto maior de informações que, ao fim e ao cabo, somente poderá ser disponibilizado pelos pais ou responsáveis das crianças, isso em face de possível conhecimento reduzido delas sobre

determinados dados – o que nem sempre, entretanto, pode corresponder à realidade, já que cada vez mais as crianças têm se adaptado ao uso prematuro de *smartphones*, *tablets* e outros dispositivos interconectados.

Outra questão interessante que ainda reside neste mesmo art. 14, §1º da LGPD diz respeito ao tratamento de dados dos adolescentes.

Da leitura expressa do dispositivo em cotejo, encontra-se somente a indicação taxativa de que caberia aos pais e responsáveis lançar o consentimento expresso apenas e somente no caso de tratamento de dados de *crianças*, silenciando sobre o consentimento no tratamento de dados de *adolescentes*. A dúvida projetada a partir disso atrela-se em saber se o silêncio do legislador, neste caso, deu-se de modo proposital ou não.

Em uma dimensão de maior proteção ao referido público de menores de idade, poder-se-ia argumentar que *adolescentes*, para a finalidade do tratamento de dados pessoais, deveriam ser equiparados à disposição expressa endereçada às *crianças*, exigindo-se também àqueles o consentimento dos pais e responsáveis detalhados no caso destas. Assim, seria possível considerar que a LGPD, em tese, verticalizou o postulado de proteção integral que o ECA reserva tanto para crianças quanto para adolescentes.

Entretanto, esta não é a conclusão expressada por parcela majoritária da doutrina especializada pela matéria. Conforme explicam Renato Opice Blum e Viviane Maldonado, essas obrigações mais restritivas de consentimento de pais e responsáveis "[...] não se aplicam a titulares a partir de 13 anos de idade, em relação aos quais será suficiente a obtenção do consentimento ordinário".[26]

Em igual medida, a Comissão Especial do Congresso Nacional responsável pela estruturação do Projeto de Lei que culminou na LGPD expediu relatório no qual aponta que a ilegalidade no tratamento de dados sem consentimento de pais e responsáveis reserva-se às "[...] crianças, abaixo de 12 anos de idade", de modo que as adolescentes o consentimento autônomo seria suficiente, cabendo a cada pai, no exercício de sua autoridade parental, o cuidado e zelo com as atividades de suas filhas e seus filhos em ambiência virtual.[27]

Disso, podem-se abrir duas possibilidades de compreensão normativa acerca de tal questão.

A primeira delas implicaria em reconhecer que, de certo modo, a disposição do art. 14, §1º da LGPD implicaria em violação ao sistema de capacidade estruturado no Código Civil, que estabelece, em seu art. 3º, *caput*, a incapacidade absoluta dos menores de dezesseis anos para os atos da vida civil e, ao seu turno, no seu art. 4º, inciso I, a capacidade relativa daqueles que conta com idade entre dezesseis e dezoito anos.[28]

Assim, se reconhecido for o consentimento para o tratamento de dados pessoais como um ato atrelado à vida civil, a LGPD permitiria a sua prática livre por pessoas que, de acordo com o Código Civil brasileiro, não possuiriam discernimento suficiente para tanto.

A segunda possibilidade, entretanto, convida à realização de um exame panorâmico das legislações aplicáveis sobre a matéria, em seu viés sistêmico.

Neste aspecto, seria possível reconhecer que a atual realidade brasileira aponta (conforme destacado nas pesquisas mencionadas acima) que os jovens têm desenvolvido com celeridade cada vez maior autonomia para o uso de plataformas digitais e aplicativos de diversas ordens. Logo, àquele grupo que, de acordo com a legislação específica (qual seja, o ECA), não seja considerado como *crianças* caberá aos pais um exercício cada vez mais atento ao poder familiar, em uma conjugação das hipóteses descritas no próprio art. 1.634 do Código Civil.

É dizer, talvez em termos mais claros, que a *Lei Geral de Proteção de Dados* assenta-se na ideia (a rigor correta) de que a mera previsão de instrumentos de proteção extensos e taxativos não dará conta da constante modificação da realidade das relações interpes-

26 OPICE BLUM, Renato; MALDONADO, Viviane Nóbrega [Coords.]. **LGPD – Lei Geral de Proteção de Dados Comentada.** 2ª Ed [livro eletrônico]. São Paulo: Thomson Reuters, 2019.

27 COMISSÃO ESPECIAL DESTINADA A PROFERIR PARECER AO PROJETO DE LEI NO 4060, DE 2012. **Relatório**. Disponível em: < https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1663305&filename=Tramitacao-PL+4060/2012>. Acesso em agosto de 2020.

28 É de se ressalvar, aqui, a modificação no sistema de capacidade civil atrelado às pessoas com deficiência, conforme estruturado na Lei nº 13.146/2015.

soais e do uso cada vez mais incessante de plataformas digitais, sendo necessário exigir daqueles que responsáveis são por pessoas em situação de vulnerabilidade por idade uma conscientização maior sobre os cuidados imprescindíveis em tal cenários, sendo eles, pais e responsáveis, convidados a participar ativamente no desenvolvimento da personalidade de seus filhos, desenvolvimento esse que cada vez mais também se faz por meio do acesso à tecnologia.

Evidente que ambas as possibilidades aqui tratadas não são mutuamente excludentes, mas há aqui a oportunidade de reconhecer uma chance para que pais e filhos transformem-se, em conjunto, como autores de suas próprias biografias, independente da presença ou existência prévia de mecanismos de proteção abrangentes – os quais, sublinhe-se, mostram-se indispensáveis em casos pontuais.

## Conclusões

Ao momento em que este estudo alcança a sua conclusão, o país assiste o provável encerramento dos avanços e recuos inerentes à entrada em vigor da *Lei Geral de Proteção de Dados*, isso ante o encaminhamento à Presidência da República, pelo Senado Federal, do Projeto de Lei de Conversão nº 34/2020, derivado, como sabido, da Medida Provisória nº 959/2020.[29]

Sem prejuízo disso, a LGPD ainda atrai discussões que envolvem questões como (in) segurança jurídica, adaptação dos destinatários da nova legislação (principalmente quanto aos gestores das grandes plataformas digitais) e, ainda, a criação concreta ou não da *Autoridade Nacional de Proteção de Dados*, peça-chave para que a LGPD e suas sanções sejam efetivadas.

Ainda que a expectativa seja intensa, não se pode ignorar que, como se deu em outros campos da ordem jurídica – tal qual as relações familiares e o Direito das Famílias –, também a tutela da privacidade e a proteção de dados pessoais dependerá de construção doutrinária e jurisprudencial, campos responsáveis por verticalizar na sociedade as disposições que constam, até o momento, na *Lei Geral de Proteção de Dados*.

O que não se pode perder de vista é que, de modo inegável, a legislação em tela vem à luz animada não apenas por um viés protetivo mas também por uma salutar premissa de autonomia à pessoa titular dos dados pessoais coletados e tratados pelas plataformas digitais que, como dito, preenchem e movimento boa parte das relações sociais e econômicas atualmente travadas.

É de vital importância destacar que hoje muito mais que ontem e mais acentuado no futuro, a identificação dos jovens e correspondência com maior intensidade pelas vias digitais, criaram um mundo privativo e de uma linguagem que só a eles tem a compreensão.

As dificuldades dos núcleos familiares em face da desestruturação de ideias e comportamentos motivou um número acentuado de separações e de relações antes não conhecidas no terreno das famílias e com isto aflorado a curiosidade a falta de acolhimento, ou de diálogo, fez com que os jovens desde a infância e concentrado na adolescência refugiassem na mundo virtual e ali se estabelecessem com premissas muitas vezes distorcidas da realidade e trazendo consequências devastadoras na personalidade, que se transforma o calvário dos que se tornaram precocemente pais, ou daqueles que já vem de uma conduta desestruturada de família primeva.

O que nos traz a reflexão para todo o obreiro do direito de família e dos que mergulham no tema voltados principalmente ao interesse da "criança e do adolescente", é esta independência desenfreada e ausente de modelos, desconhecendo resultados das condutas percursoras da carência afetiva que conduz ao caos interno. Percebemos com muita frequência que as crianças se utilizam do *YouTube* para criarem uma identidade artística o que vem sendo aplaudida pelos pais, todavia, isto enseja uma responsabilidade maior pelos responsáveis, vez que a facilidade de comunicação e aplausos virtuais proporcionam certo deleite as crianças que se tornam alvos dos mal intencionados.

Abre-se aqui, como dito acima, a chance de aproveitar uma oportunidade de que, no que diz respeito ao livre desenvolvimento da personalidade nos núcleos familiares, seja

29 UOL. Senado decide que LGPD entra em vigência agora, mas prazo depende de sanção. Disponível em: <https://www.uol.com.br/tilt/noticias/redacao/2020/08/26/senado-aprova-mp-959-mas-remove-artigo-4-e-lgpd-entra-em-vigencia-amanha.htm?cmpid=copiaecola>. Acesso em agosto de 2020.

resgatado o senso de responsabilidade e protagonismo que toda pessoa deve assumir perante sua própria vida, sua própria existência. Assim, para além da tutela legal e da solidariedade que deflui da ordem constitucional, cada pessoa pode ser timoneira de seu próprio caminho, em um espaço onde a autodeterminação informativa pode contribuir abertamente com a estruturação de laços familiares firmes e concretos.

Esse itinerário, por certo, ainda não foi concluído, e há muito por percorrer. Que não percamos o ânimo e o ímpeto de seguir com passos firmes, sempre em frente.

## Referencial Teórico


CALDERÓN, Ricardo Lucas. **Princípio da Afetividade no Direito de Família.** Rio de Janeiro: Renovar, 2013.

COMISSÃO ESPECIAL DESTINADA A PROFERIR PARECER AO PROJETO DE LEI NO 4060, DE 2012. **Relatório**. Disponível em: < https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1663305&filename=Tramitacao-PL+4060/2012>. Acesso em agosto de 2020.

COMITÊ GESTOR DA INTERNET NO BRASIL. **Pesquisa Sobre o Uso da Internet por Crianças e Adolescentes no Brasil.** TIC Kids Online Brasil. São Paulo, 2019. Disponível em: < https://cetic.br/media/docs/publicacoes/216370220191105/tic_kids_online_2018_livro_eletronico.pdf>. Acesso em julho de 2020.

CORRÊA, Rafael. Os Plúrimos Sentidos Da Privacidade E Sua Tutela: A questão da proteção de dados pessoais e sua violação na atual construção jurisprudencial brasileira. *In*: **ANIMA**. Revista Eletrônica do Curso de Direito das Faculdades Opet, v. IX, p. 1-19, 2017. Disponível em: < http://www.anima-opet.com.br/pdf/anima16/1.Os-Plurimos-Sentidos-da-Privacidade-e-sua-Tutela-Rafael-Correa.pdf>. Acesso em agosto de 2020.

DONEDA, Danilo. **Da Privacidade à Proteção de Dados Pessoais**. Rio de Janeiro: Renovar, 2006.





FRAZÃO, Ana. Plataformas digitais, *big data* e riscos para os direitos da personalidade. *In*: TEPEDINO, Gustavo; MENEZES, Joyceane Bezerra de [Coord.]. **Autonomia Privada, Liberdade Existencial e Direitos Fundamentais**. Belo Horizonte: Fórum, 2019.

INSTITUTO PLAY. (2016). **Prazer: Somos a Geração alpha**. Gente, uma conexão Globosat. Acesso em 27 de junho de 2019, disponível em: <http://gente.globosat.com.br/wp-content/uploads/2018/06/Globosat-Gente-Geracao-Alpha.pdf>. Acesso em agosto de 2020.

JÚNIOR, Marcos Ehardt *et al*. Breves notas sobre a ressignificação da privacidade. *In*: **Revista Brasileira de Direito Civil – RBDCivil**. Belo Horizonte. Vol. 16. Abr/Jun 2018. p. 35.56.

LISSARDY, Gerardo. **'Despreparada para a era digital, a democracia está sendo destruída', afirma guru do 'big data'**. Disponível em < https://www.bbc.com/portuguese/geral-39535650>. Acesso em agosto de 2020.

MAGRANI, Eduardo. **Entre Dados e Robôs**. Ética e privacidade na era da hiperconectividade. Série Pautas em Direito. Porto Alegre: Arquipélago Editorial, 2019 [livro eletrônico].

_____ **A Internet das Coisas.** Rio de Janeiro: FGV Editora, 2018 [livro eletrônico].

MARINELI, Marcelo Romão. **Privacidade e Redes Sociais Virtuais.** Sob a égide da 12.965/2014 – Marco Civil da Internet e da Lei 13.709/2019 – Lei Geral de Proteção de Dados Pessoais [livro eletrônico]. São Paulo: Thomson Reuters Brasil, 2019.

OPICE BLUM, Renato; MALDONADO, Viviane Nóbrega [Coords.]. **LGPD – Lei Geral de Proteção de Dados Comentada.** 2ª Ed [livro eletrônico]. São Paulo: Thomson Reuters, 2019.

RODOTÀ, Stefano. **A Vida na Sociedade de Vigilância**. A privacidade hoje. Rio de Janeiro: Renovar, 2008.

SANCHES, Patrícia Correa; LAMOSA, Elisabeth. **O Direito à Privacidade dos Dados na Seara do Direito das Famílias.** Artigos do Instituto Brasileiro de Direito de Família – IBDFAM. Disponível em: < https://www.ibdfam.org.br/artigos/1375/O+Direito+%C3%A0+Privacidade+dos+Dados+na+Seara+do+Direito+das+Fam%C3%ADlias>. Acesso em julho de 2020.

SCHREIBER, Anderson. Direito à privacidade no Brasil: avanços e retrocessos em 25 anos de Constituição. *In*: CLÈVE, Clémerson Merlin. **Direitos Fundamentais e Jurisdição Constitucional.** São Paulo: Editora Revista dos Tribunais, 2014. p. 183-201.

TODOROV, Tzvetan. **O Homem Desenraizado.** São Paulo: Record, 1999.

UOL. Senado decide que LGPD entra em vigência agora, mas prazo depende de sanção. Disponível em: <https://www.uol.com.br/tilt/noticias/redacao/2020/08/26/senado-aprova-mp-959-mas-remove-artigo-4-e-lgpd-entra-em-vigencia-amanha.htm?cmpid=copiaecola>. Acesso em agosto de 2020.

VAINZOF, Rony. Art. 2º *In*: OPICE BLUM, Renato; MALDONADO, Viviane Nóbrega [Coords.]. **LGPD – Lei Geral de Proteção de Dados Comentada.** 2ª Ed [livro eletrônico]. São Paulo: Thomson Reuters, 2019.

WAHLSTER, Wolfgang *et al* [Editors]. **New Horizons for a Data-Driven Economy**. Roadmap for usage and exploitation of Big Data in Europe. Springer International Publishing, 2016 [livro eletrônico].

WU, Tim. **The Attention Merchants.** The epic struggle to get inside our heads. London: Atlantic Books Ltda, 2017 [livro eletrônico].

ZUBOFF, Shoshana. **The Age of Surveillance Capitalism**. The fight for a human future at the new frontier of power. New York: Public Affairs, 2019 [livro eletrônico].



# Pequenos titulares e grandes desafios, a proteção de dados pessoais de crianças e adolescentes: um debate sobre melhor interesse, (des)equilíbrios, e lgpd a partir do episódio "*arkangel*" da série *black mirror*

*GABRIEL SCHULMAN*[30]

*LUCA SCHIRRU*[31]

*Por que os dedos murcham*

*Quando estou no banho?*

*Por que as ruas enchem*

*Quando está chovendo?*

*Quanto é mil trilhões*

*Vezes infinito?*

*(Adriana Partimpim - Oito Anos)*

**Sumário: 1. Alerta de *spoiler*: um episódio em debate. 2. Proteção de dados da criança e do adolescente: recorte proposto. 3. Marcos legais: as regras do jogo. 4. Proteção de dados de crianças e adolescentes: uma questão para adultos. 5. Considerações finais: a necessária *conexão* com os valores constitucionais.**

30 Advogado, sócio de Trajano Neto e Paciornik Advogado, Árbitro da CAMES. Doutor em Direito pela Universidade do Estado do Rio de Janeiro (UERJ). Mestre em Direito pela Universidade Federal do Paraná (UFPR). Especialista em Direito da Medicina (Universidade de Coimbra). Professor de Proteção de Dados Pessoais na Escola de Direito e Ciências Sociais da Universidade Positivo. Membro do Comitê de Saúde da OAB/PR e do Comitê Executivo de Saúde do CNJ no Paraná. Integrante do IBERC. E-mail: gabriel@schulman.com.br CV Lattes: http://lattes.cnpq.br/6784364023213630

31 Advogado especializado em Direito da Propriedade Intelectual pela PUC-Rio e integrante do escritório Baril Advogados. Doutor e Mestre em Políticas Públicas, Estratégias e Desenvolvimento (área de concentração: Inovação, Propriedade Intelectual e Desenvolvimento) pela UFRJ (PPED/IE). Pesquisador do Núcleo de Pesquisa em Direitos Fundamentais, Relações Privadas e Políticas Públicas (NUREP) e do INCT Proprietas. Professor Assistente na Universidade Positivo. Professor convidado do curso de Pós-Graduação em Direito da Propriedade Intelectual da PUC-Rio. Foi membro do Grupo de Pesquisa "Inteligência Artificial e Inclusão" do ITS-Rio e do GEDAI/UFPR. E-mail: schirru@schirru.adv.br CV Lattes: http://lattes.cnpq.br/7444096365092483

## Alerta de *spoiler*: um episódio em debate

Atenção leitor, antes de prosseguir recomendamos fortemente que assista na Netflix (serviço de *streaming*) ao episódio *Arkangel*, segundo episódio da quarta temporada da série Blackmirror, exibido pela primeira vez em 2017[32].

O episódio inicia com o parto de Sara. A mãe se mostra preocupada afinal, a bebê recém-nascida, por alguns instantes, não chora. O sentimento maternal e o desespero com a criança até o primeiro choro se revelam de forma absolutamente visceral.

Em um salto, Sara já é uma criança e, após ter perdido sua filha, a mãe Marie, decide instalar um chip para acompanhar o que acontece com a criança, ainda no início da infância. A trama então começa a provocar questionamentos. Qual o limite do cuidado que uma mãe pode ter com uma filha?

A tecnologia *Arkangel* consiste em um implante para monitorar os filhos, que permite localizá-los em tempo real, ver o que enxergam, e também embaçar de forma automática (pixelar) imagens fortes. Ao invés de limitar o que será visto na televisão, como um controle parental bastante profundo, a tecnologia permite bloquear cenas do mundo real, tal como atos de violência ou sangue.[33] Assim, como uma censura digital, esta funcionalidade, sob o argumento de proteger, restringe o acesso ao mundo.

Além disso, o sistema *Arkangel* grava as informações, o que permite saber em profundidade fatos ocorridos em momentos anteriores na vida da pessoa, temática que aliás a série já havia enfrentado no episódio *The Whole History of You.*

Como sempre, a série faz um amplo conjunto de representações e jogos de semiótica.

32 OMELETE. **Black Mirror.** Divulgado trailer de episódio dirigido por Jodie Foster. 25.11.2017. Disponível em: <https://www.omelete.com.br/series-tv/black-mirror-divulgado-trailer-de-episodio-dirigido-por-jodie-foster>.

33 GOSÁLVEZ, Patricia. Minha mãe me espiona: O inquietante no episódio de 'Black Mirror' sobre a mãe paranoica não é tanto a pergunta "você faria isso?", e sim "você já está fazendo?". **El País.** 08 fev. 2018. Disponível em: <https://brasil.elpais.com/brasil/2018/01/30/opinion/1517319479_681802.html>. CARNEIRO, Raquel. 'Árkangel', as neuras maternas no limite da obsessão. **Revista Veja.** 30 dez. 2017, Disponível em: <https://veja.abril.com.br/cultura/arkangel-as-neuras-maternas-no-limite-da-obsessao>



Na sede da empresa, um cartaz contém os dizeres *"Peace of mind"*, que remete tanto ao controle sobre o que se passa na cabeça das crianças, quanto a paz de espírito dos pais de não se preocuparem com os perigos do mundo.

Uma cena de violência, um cachorro latindo, são cenas suprimidas pelo sistema. A provocação de um mundo sem perigos, e ao mesmo tempo da hiperproteção se revela de modo delicado e ao mesmo tempo instigante.

Sara continua a crescer e, ainda com o sistema instalado durante a sua adolescência, ao não encontrar a filha, nem conseguir contato, a mãe ativa o sistema, e descobre a filha em uma relação sexual. Marie, a mãe, ao mesmo tempo sente o desconforto e o poder. A mãe segue com sua intervenção na vida da filha, ao ameaçar o rapaz com o qual Sara se relaciona. O controle extrapola o monitoramento, e passa a interferências diretas na vida, sem qualquer prévia conversa com filha.

Ao descobrir a gravação do sexo, Sara revolta-se. Termina por atacar a mãe com o próprio *tablet* utilizado como unidade de controle parental do sistema *Arkangel*. Em uma metáfora em que a violação gera a reação que a destrói, e que o mecanismo para evitar cenas fortes é utilizado para a violência,

Sara então abandona a mãe. A vigilância desmedida converte-se na extinção de qualquer forma de controle. Sara sai de casa, sem direção e aceita carona do primeiro estranho que aparece. Em uma verdadeira provocação sobre o desconhecido, sobre os riscos de não conferir maturidade e responsabilidade aos filhos. Em uma ponte, Sara sobe então em um caminhão. Aqui novas metáforas são possíveis, inclusive a possibilidade dela conhecer novos mundos, desligar-se da relação anterior, ou até estar disposta a correr riscos desnecessários, como uma reação à repressão que sofreu ao longo de sua infância e adolescência.

Estirada no chão após ser atacada com o *tablet*, a mãe não falece, o que pode sugerir a possibilidade de uma reconciliação, a derrocada da relação, ou mesmo a perda de uma conexão que ao invés de ser baseada no amor, foi construída com base no controle, e se corroeu.

O título do episódio, arcanjo na tradução para a língua portuguesa, designa o chefe dos anjos. Com nomes bíblicos nas protagonistas – Sara e Marie, o arcanjo parece remeter ao cuidado, ao anjo da guarda, mas também a onipresença das divindades em que um sistema que impede a filha Sara estar sem supervisão, em uma releitura do *Big Brother* de George Orwell e do direito de estar só.

Com *Arkangel*, Sara nunca está sozinha; está sempre na companhia da tecnologia. Não possui nem autonomia para decidir o que pode ver, nem pode ocultar o que vê ou onde está.

## Proteção de dados da criança e do adolescente: recorte proposto

Desliga-se a TV e a conexão com o pesado cenário distópico retratado em *Black Mirror*. A cena é comum, uma criança chora, os pais olham pela câmera - babá eletrônica - como está seu filho. A tecnologia, desse modo, pode ser posta a serviço da proteção e do afeto[34], ou pode converter-se em um uso desequilibrado que se mostra invasivo. Tal como um *"grain"*[35], a semente da reflexão está plantada, e implantada.

A busca pela proteção integral da criança, pela consagração de seu melhor interesse demanda então refletir sobre a proteção da intimidade, e, em sentido mais amplo, dos próprios dados pessoais, de crianças e adolescentes[36]. Como lembram Ana Carolina Brochado Teixeira e Anna Cristina de Carvalho, "as crianças e adolescentes atuais são a primeira geração cujos dados estão armazenados desde o nascimento"[37].

34 CALDERÓN, Ricardo. **Princípio da Afetividade no Direito de Família**. 2.ed. Rio de Janeiro: Forense, 2017.

35 Dispositivo capaz de armazenar e permitir o acesso a cenas da memória e que foi introduzido no episódio *"The Entire History of You"* da série *Black Mirror*.

36 Na esfera privada, observa-se "Tendo seus dados coletados desde o berço, as informações sobre o comportamento online de crianças e adolescentes são extremamente atrativas para o setor privado, pois ajudam no dtesenvolvimento de estratégias comerciais para atingir este público, que influencia as decisões de consumo de suas famílias". NEGRI, Sérgio Marcos Carvalho de Ávila; FERNANDES, Elora Raad; KORKMAZ, Maria Regina Detoni Cavalcanti Rigolon. A proteção integral de crianças e adolescentes: desafios de uma sociedade hiperconectada. In: SOARES, Fabiana de Menezes et al (Org.). **Ciência, tecnologia e inovação: políticas e leis.** Florianópolis: Editora Tribo da Ilha. 2019. p. 283-305)

37 TEIXEIRA, Ana Carolina Brochado. RETTORE, Anna Cristina de Carvalho. A autoridade parental e o tratamento de dados pessoais de crianças e adolescentes. In: TEPEDINO, Gustavo *et al.* (Coord.). **Lei geral de proteção de dados e suas repercussões no direito brasileiro.** São Paulo: Revista dos Tribunais. 2019. p. 505-530. p. 517.



É ilustrativo desta mudança social a decisão da Justiça dos Países Baixos, que concluiu que a avó não poderia manter as fotos de sua neta no *facebook38*. Em linha com o pensamento adotado neste artigo, considerou-se aplicável a norma de proteção de dados (GDPR), ainda que, tal como no direito brasileiro, à atividade doméstica sugere-se a não aplicação. Como aponta o acórdão:

O Regulamento Geral de Proteção de Dados (doravante: GDPR) protege os direitos e liberdades fundamentais das pessoas singulares e, em particular, o seu direito à proteção de dados pessoais. No entanto, o presente regulamento não se aplica ao tratamento de dados pessoais por uma pessoa singular no exercício de uma atividade puramente pessoal ou doméstica. Embora não se possa descartar que postar uma foto em uma página pessoal do Facebook se enquadre em uma atividade puramente pessoal ou doméstica, na opinião preliminar do juiz de tutela preliminar não foi suficientemente estabelecido como [réu] sua conta no Facebook ou seu Pinterst conta foi configurada ou protegida. Também não está claro se as fotos podem ser encontradas por meio de um mecanismo de busca como o Google. Além disso, com o Facebook não se pode descartar que as fotos postadas possam ser distribuídas e acabar nas mãos de terceiros. Tendo em conta estas circunstâncias, não se revelou no contexto do presente processo de medidas provisórias que exista uma atividade puramente pessoal ou doméstica de [requerido]. Isso significa que as disposições do GDPR e da Lei de Implementação do Regulamento Geral de Proteção de Dados (doravante: UAVG) se aplicam à presente disputa[39].

Vale notar que por ocasião do julgamento, apenas uma foto ainda estava nas redes sociais (*pinterest* e *facebook*), o que não foi considerado justificável, diante da falta de consentimento dos pais. Note-se deste modo a necessidade de estabelecer limites ao uso dos dados pessoais inclusive no ambiente familiar.

38 Rechtbank Gelderland. Caso n. ECLI:NL:RBGEL:2020:2521. Publicação: 13.05.2020.

39 A tradução foi feita de maneira automática por meio do mecanismo do navegador Chrome. Em outras palavras, foi executada por uma inteligência artificial. Sobre o sistema do Google, e seu aprendizado: WIGGERS, Kyle. How Google is using emerging AI techniques to improve language translation quality, **VentureBeat,** 3 jun. 2020. Disponível em: **https://venturebeat.com/2020/06/03/how-googleis-using--emerging-ai-techniques-to-improve-language-translation-quality/**

À luz de uma leitura constitucional, o reconhecimento da criança com vulnerável exige refirmar sua proteção concreta. Não se trata nem de consagrar uma autonomia irrestrita a criança, nem de, sob o argumento de proteger, permitir invasão descontrolada. Como aponta Maria Celina Bodin de Moraes, por força do princípio constitucional da solidariedade, "a vulnerabilidade da pessoa humana será tutelada, prioritariamente, onde quer que ela se manifeste".[40] Deste modo, o foco não deve recair sobre sublinhar a fragilidade (ou reproduzir estigmas), mas na imposição de deveres, salvaguardas e mecanismos de proteção. Deve-se levar em conta também a *vulnerabilidade digital,* como uma nova projeção de cuidados, que contempla os múltiplos riscos oferecidos em um mundo cada vez mais tecnológico, aos quais estão expostas as pessoas de todos os tamanhos, digo, de todas as idades.

Questionar critérios, parâmetros e espaços de proteção é, portanto, parte relevante do processo de reflexão e (re)significação da proteção de dados pessoais. Cumpre questionar por exemplo, até que idade é possível manter as filmagens? Quais os limites do cuidado e da invasão do espaço de intimidade da criança e do adolescente? Como interpretar o melhor interesse da criança[41] em relação a proteção de dados pessoais?

Trata-se de ingredientes relevantes que tornam ainda mais complexas as análises em torno da proteção de dados pessoais e, também, da própria privacidade. Em tal cenário, o presente artigo procura discutir a proteção de dados pessoais, de crianças e adolescentes, no ambiente familiar. Para tanto, problematiza-se o episódio *Arkangel*, da série *Black Mirror*. A temática expõe de forma profunda o dilema acerca dos limites entre cuidado e autonomia.[42]

40 BODIN de MORAES, Maria Celina. Vulnerabilidades nas relações familiares. O problema da desigualdade de gênero. **Cadernos da Escola Judicial do TRT da 4ª Região**, v. 3, p. 20-33, 2010. p. 26.

41 Trata-se de expressão foi consagrada na Declaração Universal dos Direitos da Criança de 1959 adotada pela Assembleia das Nações Unidas de 20 de novembro de 1959 e ratificada pelo Brasil.

42 BARBOZA, Heloisa Helena. Vulnerabilidade e cuidado: aspectos jurídico. In: PEREIRA, Tânia da Silva; OLIVEIRA, Guilherme. **Cuidado & Vulnerabilidade**. Atlas: São Paulo, 2009. BARBOZA, Heloisa Helena. O Estatuto da Criança e do Adolescente e a disciplina da Filiação no Código Civil. In: **O Melhor Interesse da Criança: um debate interdisciplinar**. Coord. Tânia da Silva Pereira. Rio de Janeiro: Renovar, 2000, p.109-113. ARANTES, Esther Maria de Magalhães. Proteção Integral à Criança e ao Adolescente: Proteção versus Autonomia. **Psicologia Clínica**, n. 2, v. 21, p. 431-450, 2009.



É importante ressaltar que a leitura aqui proposta se dá sob duas frentes: a primeira tem como referência central as legislações de proteção de dados pessoais e objetiva comentar o tratamento de dados pessoais de crianças e adolescentes por agentes de tratamento que atuam perante tal público, o que no cenário hipotético seria ilustrado pela empresa *"Arkangel"*. De outro lado, propomos algumas reflexões a respeito do papel dos pais e responsáveis no que diz respeito às interferências e medidas de monitoramento e controle de seus filhos por meio de aplicativos e dispositivos eletrônicos, bem como aos seus próprios atos de compartilhamento envolvendo as crianças e adolescentes[43].

Uma advertência relevante. Em que pese a circunstância de que a Lei Geral de Proteção de Dados Pessoais, a princípio, afaste sua incidência nas relações internas da família porque "não se aplica ao tratamento de dados pessoais" (art. 4º) "quando realizado por pessoa natural para fins exclusivamente particulares e não econômicos", uma compreensão mais ampla é necessária. Em primeiro, diante dos desafios da infância conectada. Em segundo, porque "os princípios da LGPD", na realidade configuram princípio jurídicos, cuja presença no direito brasileiro é reconhecida inclusive antes de sua entrada em vigor, como consagrou o STF[44]. A Proporcionalidade, prevenção, precaução, segurança, transparência não são normas jurídicas "apenas" da Lei Geral de Proteção de Dados Pessoais, mas do ordenamento brasileiro, e de grande utilidade para solucionar questões em matéria de proteção de dados pessoais.

43 Em perspectiva similar, destacamos o estudo de Sampaio e Fujita: "No que concerne à *internet,* percebem-se duas perspectivas que afetam negativamente a privacidade do infante: (i) a coleta e o tratamento de seus dados pessoais, que desde os primeiros passos do menor começam a perfilá-lo, a compreender seus gostos, sua atividade, suas redes, com quem se relaciona, que lugares frequenta, etc. e (ii) a disponibilização de informações e imagens, feita por ele próprio em certos casos (publicações *online* e interações com conteúdo de terceiros), mas muitas vezes por seus pais, que compartilham fotografias e vídeos – o que, em excesso, convencionou-se chamar de *sharenting*." SAMPAIO, Vinícius; FUJITA, Jorge Shiguemitsu. A privacidade da criança na internet: sharenting, responsabilidade parental e tratamento de dados pessoais. In: **Anais do 2º Congresso Internacional Information Society and Law – FMU – SP** – 6/11 a 8/11. 2019. p. 490.

44 STF. MEDIDA CAUTELAR NA AÇÃO DIRETA DE INCONSTITUCIONALIDADE 6.387 DISTRITO FEDERAL. Liminar referendada em 07.05.2020.

## Marcos legais: as regras do jogo

Ao longo deste artigo, propomos ao leitor questionamentos a respeito dos limites de acesso e tratamento de dados de menores de idade, do controle dos pais e responsáveis sobre seus filhos e suas experiências mundo afora. Questionamentos que podem ser encarados como provocações a respeito das relações familiares em uma sociedade cada vez mais conectada, ou a respeito dos limites legais de tal interferência por parte dos pais e responsáveis. A incerteza e o medo do "novo" relacionados à primeira roupagem demandam o conhecimento dos elementos que subsidiam a segunda análise. Neste sentido, dedicaremos algumas linhas para tratar dos marcos legais pertinentes ao tema.

A privacidade, e a proteção de dados pessoais[45], representam elementos dotados do maior protagonismo no cenário jurídico. Não apenas pela sua importância frente ao crescente uso de dados (pessoais), mas também pelas recentes, e fortes, emoções vivenciadas no que diz respeito à vigência da Lei Geral de Proteção de Dados Pessoais.

Apesar de a entrada em vigor LGPD representar uma importante conquista no que diz respeito à proteção da privacidade, a regulação a respeito do tratamento de dados pessoais antecede a sua promulgação[46]. Para este item, abordaremos disposições constantes da Constituição Federal de 1988, da Convenção sobre os Direitos da Criança, do Código Civil de 2002, do Marco Civil da Internet, do Estatuto da Criança e do Adolescente e da Lei Geral de Proteção de Dados Pessoais, sempre privilegiando as relações envolvendo o tratamento de dados de crianças e adolescentes.

45 DONEDA, Danilo. **Da privacidade à proteção de dados pessoais.** Rio de Janeiro: Renovar, 2006.

46 MULHOLLAND, Caitlin Sampaio. Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da lei geral de proteção de dados (Lei 13.709/18). **Revista de Garantias Fundamentais,** Vitória, v. 19, n. 3, p. 159-180, set./dez. 2018.



A Constituição Federal de 1988 traz como garantias fundamentais a inviolabilidade da intimidade, da vida privada[47] (art. 5º, X), do domicílio[48] (art. 5º, XI) e do sigilo de correspondência[49] (art. 5º, XII). Considerando o tema aqui proposto, importante ressaltar que tais direitos fundamentais, e os demais direitos humanos e fundamentais inerentes à pessoa humana, são constitucionalmente garantidos aos pais e também a seus filhos[50], crianças e adolescentes, sendo dever daqueles, do Estado e da sociedade como um todo, assegurar o seu exercício pelos menores, conforme se extrai da interpretação dos arts. 3º e 98 da Lei nº 8.069/90 (Estatuto da Criança e do Adolescente)[51] e do art. 227 da Constituição Federal de 1988.

47 CF88, Art. 5º: "Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: [...] 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;".

48 CF88, Art. 5º: "Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: [...] XI - a casa é asilo inviolável do indivíduo, ninguém nela podendo penetrar sem consentimento do morador, salvo em caso de flagrante delito ou desastre, ou para prestar socorro, ou, durante o dia, por determinação judicial;(Vide Lei nº 13.105, de 2015) (Vigência)".

49 CF88, Art. 5º: "Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: [...] 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"

50 CF88: "Art. 227. É dever da família, da sociedade e do Estado assegurar à criança, ao adolescente e ao jovem, com absoluta prioridade, o direito à vida, à saúde, à alimentação, à educação, ao lazer, à profissionalização, à cultura, à dignidade, ao respeito, à liberdade e à convivência familiar e comunitária, além de colocá-los a salvo de toda forma de negligência, discriminação, exploração, violência, crueldade e opressão.

51 Estatuto da Criança e do Adolescente , Art. 3º: "A criança e o adolescente gozam de todos os direitos fundamentais inerentes à pessoa humana, sem prejuízo da proteção integral de que trata esta Lei, assegurando-se-lhes, por lei ou por outros meios, todas as oportunidades e facilidades, a fim de lhes facultar o desenvolvimento físico, mental, moral, espiritual e social, em condições de liberdade e de dignidade." [...] "Art. 98. As medidas de proteção à criança e ao adolescente são aplicáveis sempre que os direitos reconhecidos nesta Lei forem ameaçados ou violados: [...] Parágrafo único. São também princípios que regem a aplicação das medidas: [...] V - privacidade: a promoção dos direitos e proteção da criança e do adolescente deve ser efetuada no respeito pela intimidade, direito à imagem e reserva da sua vida privada;"

Em consonância com o que foi exposto acima, destaca-se também a Convenção sobre os Direitos da Criança, promulgada pelo Decreto n. 99.170/1990 e que determina a necessidade de observância do interesse maior da criança como parâmetro central para a tomada de decisões por instituições públicas e privadas[52], sendo vedada qualquer interferência de caráter arbitrário ou ilegal em sua vida privada[53].

Sendo assim, a criação, a educação e a exigência da obediência e respeito, deveres constantes no Estatuto da Criança e do Adolescente (e.g. art. 22) e no Código Civil de 2002 (art. 1.634) não devem ser exercidos de maneira ilimitada, sob pena de suspensão do poder familiar[54], dentre outras sanções aplicáveis.

No que diz respeito à história envolvendo Sara e Marie em *Arkangel*, por exemplo, é lícita, e comum, a utilização de programas de computador para o exercício de controle parental de conteúdo acessado por crianças e adolescentes no ambiente online, desde que nos limites das normas aqui referenciadas[55]. No cenário hipotético ilustrado em *Black Mirror*, e sob a Lei Geral de Proteção de Dados (art. 14, §§ 1º e 2º), o uso dos dispositivos *Arkangel* compreende coleta e outras atividades tratamento de dados, demandando a obtenção consentimento específico por parte de Marie, que também deverá ter acesso a todas as informações a respeito dos dados coletados de Sara, bem como a sua destinação.

52 Decreto 99.170/90: "Artigo 3. 1. Todas as ações relativas às crianças, levadas a efeito por instituições públicas ou privadas de bem estar social, tribunais, autoridades administrativas ou órgãos legislativos, devem considerar, primordialmente, o interesse maior da criança.".

53 Decreto 99.170/90: "Artigo 16. 1. Nenhuma criança será objeto de interferências arbitrárias ou ilegais em sua vida particular, sua família, seu domicílio ou sua correspondência, nem de atentados ilegais a sua honra e a sua reputação. 2. A criança tem direito à proteção da lei contra essas interferências ou atentados.".

54 CC2002, Art. 1.637. "Se o pai, ou a mãe, abusar de sua autoridade, faltando aos deveres a eles inerentes ou arruinando os bens dos filhos, cabe ao juiz, requerendo algum parente, ou o Ministério Público, adotar a medida que lhe pareça reclamada pela segurança do menor e seus haveres, até suspendendo o poder familiar, quando convenha. Parágrafo único. Suspende-se igualmente o exercício do poder familiar ao pai ou à mãe condenados por sentença irrecorrível, em virtude de crime cuja pena exceda a dois anos de prisão."

55 Diz o art. 29 do Marco Civil da Internet: "Art. 29. O usuário terá a opção de livre escolha na utilização de programa de computador em seu terminal para exercício do controle parental de conteúdo entendido por ele como impróprio a seus filhos menores, desde que respeitados os princípios desta Lei e da Lei nº 8.069, de 13 de julho de 1990 - Estatuto da Criança e do Adolescente. Parágrafo único. Cabe ao poder público, em conjunto com os provedores de conexão e de aplicações de internet e a sociedade civil, promover a educação e fornecer informações sobre o uso dos programas de computador previstos no caput, bem como para a definição de boas práticas para a inclusão digital de crianças e adolescentes.".



Além das medidas de controle parental autorizadas pelo Marco Civil da Internet, voltadas para o material acessado online, o Estatuto da Criança e do Adolescente estabelece restrições a emissoras de rádio e televisão, empresas que atuam na venda e exibição de materiais de vídeo, revistas e publicações para que, no exercício de suas atividades, não venham expor crianças e adolescentes a conteúdo impróprio ou inadequado[56].

Por fim, e ainda sobre o tratamento de dados pessoais de crianças e adolescentes, há que se atentar para a criação de bancos de dados e cadastros de consumidores, sujeito às regras do Código de Defesa do Consumidor[57].

Se valendo da dualidade inerente aos questionamentos que orbitam este texto, e com apoio no disposto no caput do art. 14 da LGPD, cumpre questionar: será que o tratamento de dados pessoais de Sara foi realizado em seu melhor interesse?

## Proteção de dados de crianças e adolescentes: uma questão para adultos

A proteção da criança se mostra, neste passo, essencial, em 21 de janeiro de 2020, o *Information Commissioner's Office* (ICO), autoridade inglesa, publicou o documento *"Age appropriate design: a code of practice for online services"*[58], um estatuto com 15 padrões que os serviços online devem atender para proteger a privacidade das crianças.

56 Arts, 77 e seguintes do Estatuto da Criança e do Adolescente.

57 Arts; 42, 43, 44, 72 e 73, por exemplo.

58 UNITED KINGDOM. INFORMATION COMMISSIONER'S OFFICE (ICO). **Age appropriate design: a code of practice for online services**. ICO children's code. Londres: ICO. Setembro de 2020. Disponível em: <https://ico.org.uk/media/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services-2-1.pdf>.

Em que pese o Código do ICO não possuir o mesmo escopo de aplicação da LGPD[59], representa uma importante referência no que diz respeito à adequação de sistemas e processos às normas de proteção de dados que são propostas pela GDPR e que podem se comunicar com as obrigações constantes da nossa legislação de proteção de dados pessoais[60]. Além disso, o fato de ser fortemente influenciada pela Convenção sobre os Direitos da Criança, promulgada pelo Decreto n. 99.170/90, representa uma aproximação relevante com o ordenamento jurídico brasileiro[61]. Assim, a análise do documento se mostra bastante útil e justifica-se diante da falta de um marco mais denso no ordenamento brasileiro.

As configurações devem ser padrão alta e técnicas de estimulo (*nudges*)[62] devem ser empregadas para evitar alterações de configurações pelas crianças. Configurações de localização devem ser desativas por padrão (*privacy by design e privacy by default*)[63].

A abordagem da ICO, muito útil para o direito brasileiro, adota a idade como um dos critérios na avaliação de risco e proporcionalidade. Trata-se de perspectiva que se harmoniza, de modo mais refinado, com o reconhecimento do progressivo amadurecimento

59 Sobre a aplicação do Código, destaca-se o trecho de ICO, 2020, p. 18: "This code is issued under the DPA 2018. The DPA 2018 applies to online services based in the UK. It also applies to online services based outside the UK that have a branch, office or other 'establishment' in the UK, and process personal data in the context of the activities of that establishment. The DPA 2018 may also apply to some other services based outside the UK even if they don't have an establishment in the UK. If the relevant establishment is outside the European Economic Area (EEA), the DPA 2018 still applies if you offer your service to users in the UK, or monitor the behaviour of users in the UK. The code applies if that service is likely to be accessed by children."

60 Em ICO, 2020, p. 10: "How does this code support data protection compliance? The UK data protection regime is set out in the Data Protection Act 2018 (DPA 2018) and the GDPR. This regime requires you to take a risk-based approach when you use people's data, based on certain key principles, rights and obligations. This code supports compliance with those general principles by setting out specific protections you need to build in when designing online services likely to be accessed by children,[...]"

61 ICO, 2020, p. 3: "This code will lead to changes in practices that other countries are considering too. It is rooted in the United Nations Convention on the Rights of the Child (UNCRC) that recognises the special safeguards children need in all aspects of their life. Data protection law at the European level reflects this and provides its own additional safeguards for children."

62 MONTELEONE, Shara, *et. al.* **Nudges to Privacy Behaviour:** Exploring an Alternative Approach to Privacy Notices, European Union 2015.

63 ICO, 2020.



da criança e do adolescente, pequeno em tamanho e enorme em direitos e formas de tutela. Esse reconhecimento do espaço de autodeterminação se pode extrair do próprio teor da LGPD, quando estabelece em seu art. 14 a participação da criança e do adolescente em atos decisórios, com regras distintas para cada fase da vida.

O consentimento no mundo digital inclusive se mostra em si um desafio. Adotar a capacidade civil é insuficiente, seja porque há diversos atos não exatamente patrimoniais, seja porque a própria autonomia dos atos existenciais se mostra complexa[64].

Crianças e adolescentes não possuem direitos menores do que adultos, e sua proteção deve ser ainda maior. Direitos como acessar dados e retificar, inclusive em confronto com as manifestações de seus pais são interesses juridicamente relevantes e que não se solucionam pelos tradicionais mecanismos de representação jurídica. Ao contrário, devem estar atentos à proteção de dados como direito fundamental[65] e ao melhor interesse da criança e adolescente como baliza em sua aplicação, como decorrência da matriz da solidariedade constitucional onde este princípio encontra um dos seus fundamentos[66].

64 SCHULMAN, Gabriel. **Internação Forçada, Saúde Mental e Drogas**: é possível internar contra a vontade? Indaiatuba: Editora Foco, 2020. MATOS, Mafalda Francisco. **O problema da (ir)relevância do consentimento dos menores em sede de cuidados médicos terapêuticos (uma perspectiva jurídico-penal).** Coimbra Editora. 1ª Edição, julho 2013. MARTINS-COSTA, Judith. Capacidade para consentir e esterilização de mulheres tornadas incapazes pelo uso de drogas: notas para uma aproximação entre a técnica e a reflexão bioética. In: MARTINS COSTA, Judith; MOLLER, Letícia Ludwig. (Org.). **Bioética e Responsabilidade**. Rio de Janeiro: Forense, 2009. p. 299-346. TEIXEIRA, Ana Carolina Brochado. Integridade psíquica e capacidade de exercício. **Revista Trimestral de Direito Civil**, vol. 33, 2008. PEREIRA, André Gonçalo Dias. A capacidade para consentir: um novo ramo da capacidade jurídica. Separata da Faculdade de Direito da Universidade de Coimbra**. Comemorações dos 35 anos do Código Civil e dos 25 anos da reforma de 1977.** Coimbra: Coimbra Editora: 2006. ROSS, Lainie Friedman. Moral Grounding for the Participation of Children as Organ Donors. **The Journal of Law, Medicine & Ethics, 1993**, 21(2):251-257.

65 Nesse sentido, Rodotà: "considerando la protezione dei dati personali come un autonomo diritto fondamentale, distinto dalla tradizionale idea di privacy". RODOTÀ, Stefano. **Il diritto di avere diritti**, Roma-Bari, Laterza 2012. p. 80.

66 LÔBO, Paulo Luiz Netto. O princípio constitucional da solidariedade nas relações de família. In: CONRADO, Marcelo (Org.). **Direito Privado e Constituição:** ensaios para uma recomposição valorativa da pessoa e do patrimônio. Curitiba: Juruá, 2009. p. 327

As orientações da autoridade inglesa, incluem:

- Best interests of the child
- Data protection impact assessments
- Age appropriate application
- Transparency
- Detrimental use of data
- Policies and community standards
- Default settings
- Data minimisation
- Data sharing
- Geolocation
- Parental controls
- Profiling
- Nudge techniques
- Connected toys and devices
- Online tools

Dentre os padrões constantes do documento da ICO, as "configurações padrão" ("*default settings*" ou "*privacy by default*"[67]) assumem papel relevante, uma vez que acabam por ditar os parâmetros que devem ser adotados quando da interpretação das demais, tomando sempre como norte o critério do "alto grau de privacidade"[68]. A adoção dessa orientação implica, por exemplo, trabalhar com um padrão em que algumas funcionalidades de um aplicativo devam estar, a princípio, desativadas, como é o caso da Geolocalização e do Perfilamento *(profiling)*[69].

67 CAVOUKIAN, Ann. **Privacy by Design:** The 7 Foundational Principles. August, 2009.
68 Tradução nossa. Texto original: "high privacy". ICO, 2020, pp. 4-7.
69 Em ICO, 2020, p. 7.



Embora assuma papel de destaque perante as outras orientações, o "alto grau de privacidade" relacionado às "configurações padrão" não pode deixar de considerar os melhores interesses da criança, estes tomados como referência central para a interpretação de todos os demais padrões[70], o que é verificado expressamente em outros itens do Código, tais como Geolocalização ("*Geolocation*")[71], Compartilhamento de Dados ("*Data Sharing*")[72] e Perfilamento ("*Profiling*")[73].

Não apenas é necessário que as empresas que ofereçam brinquedos e dispositivos conectados ("*Connected toys and devices*")[74] assim o façam sob os padrões impostos pelo documento[75], mas também que promovam os meios necessários para que o titular de dados "exerça seus direitos relacionados à proteção de dados e relate suas preocupações" [76] ("*Online Tools*"), sempre atuando com Transparência e de acordo com os padrões existentes ("*Policies and community standards*")[77]. Ainda, o texto com as orientações demonstra preocupação com o direito da criança de se informar a respeito da privacidade e do uso seus dados pessoais, inclusive no que diz respeito ao monitoramento de sua localização ("*Geolocation*") ou do conteúdo a que está tendo acesso ("*Parental Controls*")[78].

70 Neste sentido, em ICO, 2020, p. 10: "The code incorporates the key principle from the UNCRC that the best interests of the child should be a primary consideration in all actions concerning children. It also aims to respect the rights and duties of parents, and the child's evolving capacity to make their own choices".
71 Em ICO, 2020, p. 7: "Geolocation: Switch geolocation options off by default (unless you can demonstrate a compelling reason for geolocation to be switched on by default, taking account of the best interests of the child). Provide an obvious sign for children when location tracking is active. Options which make a child's location visible to others must default back to 'off' at the end of each session."
72 Em ICO, 2020, p. 7. "Data sharing: Do not disclose children's data unless you can demonstrate a compelling reason to do so, taking account of the best interests of the child."
73 Em ICO, 2020, p. 7: "Profiling: Switch options which use profiling 'off' by default (unless you can demonstrate a compelling reason for profiling to be on by default, taking account of the best interests of the child). Only allow profiling if you have appropriate measures in place to protect the child from any harmful effects (in particular, being fed content that is detrimental to their health or wellbeing)."
74 LEAL, Livia Teixeira. Internet of toys: os brinquedos conectados à internet e o direito da criança e do adolescente. **Revista Brasileira de Direito Civil – RBDCivil**, Belo Horizonte, vol. 12, p. 175-187, abr./jun. 2017.
75 Em ICO, 2020, p. 8: "Connected toys and devices: If you provide a connected toy or device ensure you include effective tools to enable conformance to this code"
76 Tradução nossa. Texto original em ICO, 2020, p. 8: "Online tools: Provide prominent and accessible tools to help children exercise their data protection rights and report concerns"
77 Em ICO, 2020, p. 7: "Uphold your own published terms, policies and community standards (including but not limited to privacy policies, age restriction, behaviour rules and content policies)."
78 ICO, 2020, p. 7-8. Em ICO, 2020, p. 7: "Parental controls: If you provide parental controls, give the child age appropriate information about this. If your online service allows a parent or carer to monitor their child's online activity or track their location, provide an obvious sign to the child when they are being monitored."

Em contraste com tais premissas, estudos demonstram que brinquedos conectados terminam por serem pouco claros, tanto para os pais, quanto para as crianças. A clareza sobre a aptidão para gravar, a disponibilidade do que foi gravado para os pais, e outros problemas na interação das crianças, exige compreender os diferentes modelos mentais da infância e adolescência[79],

Apesar de o ordenamento jurídico brasileiro, no art. 29 do Marco Civil da Internet, dispor a respeito do controle parental, não prevê de maneira expressa a respeito da necessidade de manter a criança informada a respeito de tal controle. A despeito da necessária garantia da privacidade de crianças e adolescentes, as medidas devem considerar o seu melhor interesse, o que, perpassaria por uma sensível análise particular e que considere a idade, o contexto no qual são aplicadas tais medidas e as tecnologias disponíveis. Inclusive, o Código traz como uma das orientações a consideração das diferentes idades/faixas de idade quando da implementação das medidas de privacidade e proteção de dados pessoais, fornecendo também informações complementares a respeito das peculiaridades inerentes às diferentes faixas de desenvolvimento ("*age appropriate application*")[80].

O exemplo acima, sobre a relação entre o disposto no Marco Civil da Internet a respeito do controle parental e os padrões propostos pelo ICO, representa a oportunidade de olhar atentamente para os padrões sob análise de maneira a buscar possíveis correspondências, ainda que parciais em nosso ordenamento jurídico.

Sem qualquer intenção de exaurir o tema, e de maneira a ilustrar como tais orientações se comunicam com os marcos legais brasileiros aqui referenciados, construímos a tabela abaixo, que relaciona as orientações da ICO com normas vigentes no direito brasileiro:

79 MCREYNOLDS, Emily, *et al.* **Toys that listen**: A study of parents, children, and internet-connected toys. Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems. Denver, CO, USA: ACM, 5197-207.

80 ICO, 2020, p. 32-33: "What do you mean by 'age appropriate application'? This means that the age range of your audience and the different needs of children at different ages and stages of development should be at the heart of how you design your service and apply this code.[...] Further information about relevant capacities, needs, skills and behaviours at each stage is set".

| Padrões ICO (2020, p. 7-8) | Norma interna |
|---|---|
| "**Best interests of the child**: The best interests of the child should be a primary consideration when you design and develop online services likely to be accessed by a child." | Art. 227, CF; Art. 14, LGPD; Art. 98, Parágrafo Único, IV e 100, Estatuto da Criança e do Adolescente Art. 3º (1) do Decreto 99.710/90; Art. 16 do Decreto 99.710/90 |
| "**Data protection impact assessments**: Undertake a DPIA to assess and mitigate risks to the rights and freedoms of children who are likely to access your service, which arise from your data processing. Take into account differing ages, capacities and development needs and ensure that your DPIA builds in compliance with this code." | Art. 5º, XVII, LGPD; Art. 38, LGPD; Art. 55-J, XII, LGPD |
| "**Age appropriate application**: Take a risk-based approach to recognising the age of individual users and ensure you effectively apply the standards in this code to child users. Either establish age with a level of certainty that is appropriate to the risks to the rights and freedoms of children that arise from your data processing, or apply the standards in this code to all your users instead." | Art. 6º, I e II, LGPD; Art. 7º, XII, MCI; |
| "**Transparency**: The privacy information you provide to users, and other published terms, policies and community standards, must be concise, prominent and in clear language suited to the age of the child. Provide additional specific 'bite-sized' explanations about how you use personal data at the point that use is activated." | Art. 6º, VI, LGPD; Art. 14, § 2º LGPD; Art. 7º, VIII, XI, MCI; |

| | |
|---|---|
| "**Detrimental use of data**: Do not use children's personal data in ways that have been shown to be detrimental to their wellbeing, or that go against industry codes of practice, other regulatory provisions or Government advice." | Art. 6º, IX, LGPD; Art. 5º, Estatuto da Criança e do Adolescente; |
| "**Policies and community standards**: Uphold your own published terms, policies and community standards (including but not limited to privacy policies, age restriction, behaviour rules and content policies)." | Art. 14, § 2º LGPD; Art. 7º, VIII, MCI; |
| "**Default settings**: Settings must be 'high privacy' by default (unless you can demonstrate a compelling reason for a different default setting, taking account of the best interests of the child)" | Art. 3º, II e III, MCI; Art. 98, Parágrafo Único, V, Estatuto da Criança e do Adolescente.; Art. 5º, X, CF88, Art. 227, CF88 |
| "**Data minimisation**: Collect and retain only the minimum amount of personal data you need to provide the elements of your service in which a child is actively and knowingly engaged. Give children separate choices over which elements they wish to activate." | Art. 6º, III, LGPD; Art. 14, § 4º, LGPD; |
| "**Data sharing**: Do not disclose children's data unless you can demonstrate a compelling reason to do so, taking account of the best interests of the child." | Art. 6º, I, II e III, LGPD; Art. 7º, VII, MCI; |
| "**Geolocation**: Switch geolocation options off by default (unless you can demonstrate a compelling reason for geolocation to be switched on by default, taking account of the best interests of the child). Provide an obvious sign for children when location tracking is active. Options which make a child's location visible to others must default back to 'off' at the end of each session." | Art. 14, § 6º, LGPD; Art. 98, Parágrafo Único, V, Estatuto da Criança e do Adolescente. |
| "**Parental controls**: If you provide parental controls, give the child age appropriate information about this. If your online service allows a parent or carer to monitor their child's online activity or track their location, provide an obvious sign to the child when they are being monitored." | Art. 14, § 6º, LGPD; Art. 29, MCI; |
| "**Profiling**: Switch options which use profiling 'off' by default (unless you can demonstrate a compelling reason for profiling to be on by default, taking account of the best interests of the child). Only allow profiling if you have appropriate measures in place to protect the child from any harmful effects (in particular, being fed content that is detrimental to their health or wellbeing)." | Art. 6º, VII, LGPD; Art. 20, § 1º, LGPD; Art. 12, § 2º, LGPD |
| "**Nudge techniques**: Do not use nudge techniques to lead or encourage children to provide unnecessary personal data or weaken or turn off their privacy protections." | Art. 6º, III, LGPD |
| "**Connected toys and devices**: If you provide a connected toy or device ensure you include effective tools to enable conformance to this code." | Todos os dispositivos legais referenciados nesta tabela se aplicam. |
| "**Online tools**: Provide prominent and accessible tools to help children exercise their data protection rights and report concerns." | Art. 14, § 6º, LGPD; Art. 18, LGPD; Art. 7º, VIII, XI, MCI; Art. 29, MCI; |

A partir do quadro acima, é possível observar que as diretrizes da ICO servem como interessante parâmetro para o direito brasileiro. Uma matriz nacional pode acrescentar o reconhecimento da vulnerabilidade e da autonomia progressiva da criança e do adolescente.

Esta percepção impõe um reconhecimento da necessidade de uma análise que seja feita de maneira dinâmica e contextual, como é inerente às relações existenciais[81]. Sob a perspectiva do direito de família, a perspectiva do cuidado deve levar em conta a passagem de um modelo autoritário a um modelo dialógico,[82] que reconhece o espaço de autonomia progressiva da criança e do adolescente.[83]

O próprio apoio dos pais é fundamental no processo de compreensão da exposição dos dados (fotos, imagens, vídeos, sentimentos) em espaços públicos virtuais[84], demonstrando a importância de uma educação para um mundo cada vez mais digital, para todas as idades[85]. Para ilustrar, um levantamento feito com mais de 800 jovens demonstra que em 2012, 91 dos jovens postou fotos suas nas mídias sociais, em relação a 79% em 2006; o nome da escola era identificado por 71% e seu endereço de e-mail por mais da metade[86].

Considerando o cenário proposto pelo episódio *Arkangel*, nos dedicamos agora a uma análise pontual sob as orientações da ICO. Para tanto, assumiremos a premissa de que a empresa (*"Arkangel"*) fornece tais produtos e serviços de acordo com as normas de proteção de dados pessoais no que diz respeito à transparência e aos padrões adotados em seus documentos que tratem da privacidade de seus usuários (itens *"Transparência"* e *"Padrões de Comunidade e Políticas"*)[87]. A parte dos itens aqui referenciados, o tratamento de dados ali realizado parece afrontar boa parte das orientações transmitidas pelo documento do ICO.

81 PERLINGIERI, Pietro. O **direito civil na legalidade constitucional**. Rio de Janeiro: Renovar, 2008. KONDER, Carlos Nelson. Vulnerabilidade Patrimonial e Vulnerabilidade Existencial: por um sistema diferenciador. **Revista de Direito do Consumidor**, v. 99, p. 101-123, 2015.

82 OLIVEIRA, Ligia Ziggioti de. **Cuidado como valor jurídico**: crítica aos direitos da infância a partir do feminismo. Tese. (Doutorado em Direito). UFPR, 2019, p. 72.

83 TEFFÉ, Chiara A. Spadaccini de. Proteção de dados de crianças e adolescentes. **Revista do Advogado**, v. 39, 2019.

84 LIVINGSTONE, Sonia; STOILOVA, Mariya; NANDAGIRI, Rishita. **Children's data and privacy online.** Growing up in a digital age an evidence review. United Kingdom: ICO, LSE. December 2018. p. 28.

85 Pesquisas mostram que há variações culturais e de gerações que influenciam a maneira como os dados são revelados pelos titulares. MONTELEONE, Shara, *et. al.* **Nudges to Privacy Behaviour:** Exploring an Alternative Approach to Privacy Notices, European Union 2015. p. 30.

86 MADDEN, Mary, *et al.* **Teens, social media, and privacy.** Washington, DC: Pew Research Center's Internet & American Life Project. 2013. Disponível em <https://cyber.harvard.edu/publications/2013/teens_socialmedia_privacy>.

87 ICO, 2020, p. 7.



De maneira geral, o controle exercido por Marie evidencia que o tratamento de dados e a utilização da tecnologia *Arkangel* definitivamente não se deu de acordo com "os melhores interesses da criança" (*"Best interests of the child"*)[88], ou de maneira a não prejudicar – ainda que sem intenção – a criança/adolescente (*"Detrimental use of data"*)[89]. Nota-se também que não foram considerados critérios de razoabilidade e proporcionalidade no que diz respeito ao tratamento de dados e a idade de Sara, o que resta evidente quando da coleta de dados de momentos da vida social de Sara quando adolescente (*"Age appropriate application"*) [90] e que também transparece quando da utilização de tecnologias de geolocalização sem considerar os interesses de Sara, e sem que esta fosse notificada sobre tal monitoramento[91].

Ao longo do episódio também é observado que não existe qualquer preocupação com a minimização do tratamento de dados, sendo ideal que os dados e imagens processadas sob comando de Marie fossem apenas aqueles absolutamente necessários para a que a mãe pudesse ter conhecimento de uma situação de exposição a um risco além daquele considerado normal para uma criança ou adolescente[92] (tomar um susto com o latido de um cachorro, comer muitos biscoitos, ou assistir uma cena de violência em um filme).

O episódio, na linha proposta pela série, trabalha com um cenário distópico, de exageros (até então) no que concerne à relação entre os humanos e a tecnologia. Não obstante, acaba por fornecer importantes reflexões no que diz respeito aos limites que devem ser considerados pelos pais e responsáveis no que diz respeito ao monitoramento de seus filhos. Até que ponto Marie poderia ter acesso aos dados pessoais de Sara? É razoável ter acesso a um simples alerta de que Sara consumiu substâncias ilícitas ou

88 ICO, 2020, p. 7.

89 ICO, 2020, p. 7.

90 ISO, 2020, p. 7: "Age appropriate application: Take a risk-based approach to recognising the age of individual users and ensure you effectively apply the standards in this code to child users. Either establish age with a level of certainty that is appropriate to the risks to the rights and freedoms of children that arise from your data processing, or apply the standards in this code to all your users instead.

91 ICO, 2020, p. 7: "Geolocation: Switch geolocation options off by default (unless you can demonstrate a compelling reason for geolocation to be switched on by default, taking account of the best interests of the child)."

92 ICO, 2020, p. 7: "Data minimisation: Collect and retain only the minimum amount of personal data you need to provide the elements of your service in which a child is actively and knowingly engaged. Give children separate choices over which elements they wish to activate."

com restrições de uso? O monitoramento por vídeo deve ser comunicado a sua filha? A funcionalidade de geolocalização pode ser utilizada enquanto mais nova, até mesmo considerando o seu rápido desaparecimento no início do episódio?

Se *"Arkangel"* trouxe reflexões a respeito das consequências trágicas do controle exagerado da vida dos filhos por parte dos pais, é importante que não haja um desequilíbrio na balança para o outro lado, da proposição de uma privacidade absoluta das crianças. É fundamental que as regras atinentes à proteção de dados pessoais e que venham a conceder autonomia decisória a estas e também as orientações do ICO, sejam sempre interpretadas à luz dos melhores interesses da criança. Sob tais interesses, defendemos que há a necessidade de, principalmente, se considerar o contexto sob análise, o que envolve, por exemplo, a idade e a condição psíquica da criança de tomar determinadas decisões, não sendo aplicável a mesma liberdade e privacidade concedida a um adolescente de 16 anos, a uma criança de 5 anos[93].

Sob a perspectiva do tratamento de dados pessoais, a partir da legislação de proteção de dados vigente, um exemplo de uma situação em que a autonomia da criança deverá ser limitada no que diz respeito à sua posição a respeito do tratamento de dados pessoais é aquela em que o tratamento é fundamental para a própria saúde e segurança da criança, não apenas no fornecimento de um determinado serviço, mas também na identificação e combate de situações de abusos cometidos em ambiente virtual[94].

Assim, interpretar as orientações, e os demais dispositivos protetivos da criança, sob os seus melhores interesses é não apenas evitar o sufocamento de todas as suas experiências sadias e dolorosas que esta certamente viverá e que são indispensáveis para o

93 À título de exemplo, transcreve-se trecho adicional de ICO,2020, p. 39: "However, in many cases a-one-size-fits-all approach does not recognise that children have different needs at different stages of their development. For example, a pre-literate or primary school child might need to be actively deterred from changing privacy settings without parental input, whereas a teenager might be better supported by clear and neutral information which helps them make their own informed decision."

94 Em ICO, 2020, p. 50: "There may also be some other limited types of processing where it is not appropriate to offer a privacy setting. For example, if you need to process a child's personal data in order to meet a legal obligation (such as a child protection requirement) or to prevent child sexual exploitation and abuse online. It is then not appropriate to offer them a choice over whether their personal data is processed for this purpose or not."



seu crescimento, mas também saber quando e como limitar as suas escolhas e opções de maneira proporcional à sua faixa etária.

## Considerações finais: a necessária *conexão* com os valores constitucionais

No jogo entre autonomia e vulnerabilidade, a proteção das crianças e adolescentes não se resolvem de maneira simples. Pais devem acompanhar a atividade dos filhos, mas é preciso refletir sobre um espaço de intimidade.

Na medida em que no fluxo do tempo, o futuro já chegou, o *controle do controle* precisa ser revisitado de maneira a enfrentar novas tecnologias que desafiam nosso direito, nossa ética[95] e quiçá até nossa imaginação. Nesse passo, observa-se que as transformações da realidade (e do virtual) criam um profundo abismo na regulação jurídica. Temas como Internet da Coisas, Algoritmos, Brinquedos Conectados, desafiam os limites de institutos como o Direito Civil.

A despeito do vácuo legislativo, e das zonas cinzentas, a Lei Geral de Proteção de Dados Pessoais é parâmetro útil na interpretação de relações interfamiliares, assim como as diretrizes da ICO. Mais do que definir uma norma "mais importante" aplicável, procurou-se identificar diretrizes centrais na proteção da criança e do adolescente.

Contudo, ainda que se proponha um *Black Mirror* às avessas, em que a tecnologia opera apenas em benefício do ser humano e que empresas estão em absoluta adequação no que diz respeito aos padrões de privacidade e às legislações de proteção de dados pessoais, ainda existem ameaças, mesmo que não intencionais, à privacidade da criança.

O universo de riscos inclui a esfera familiar. Nesse sentido, uma das ameaças é a prática de *sharenting*, que consiste no compartilhamento de conteúdo ilustrando a criança pelos seus pais e responsáveis em suas redes sociais, o que, por si só, não traria maio-

95 Nas palavras de Hans Jonas: "Care for the future of mankind is the overruling duty of collective human action in the age of the technical civilization that has become 'almighty,' if not in its productive then at least in its destructive potential. This care must obviously include care for the future of all nature on this planet as a necessary condition of man's own". JONAS, Hans. **Responsibility Today: The Ethics of an Endangered Future**. Social Research, v. 43, n. 1, abr. 1976.

res riscos[96]. Entretanto, o *sharenting* pode assumir formas capazes de expor a criança em demasia, conforme análise de Sampaio e Fujita:

> *Há, entretanto, duas modalidades de sharenting com o potencial de causar muito mais danos às crianças: (i) a exploração comercial de sua imagem, que vem se tornando comum na web, por meio de blogueiros e youtubers mirins, que auferem renda com anúncios, publicações pagas, patrocínio, etc. – o que já existia nos meios televisivo e musical, por exemplo, mas que, agora, conta com a possibilidade de interação com outros internautas, entre os quais há usuários maliciosos, trolls, entre outros -, e (ii) fotografias e vídeos pretensamente bem humorados ou humilhantes (punitivos) que expõem os menores em situações vexatórias, que acabam, intencionalmente ou não, viralizando nas redes sociais e divertindo milhares de internautas à custa da vergonha do infante.*[97]

Já em *"Arkangel"* era possível a minimização da exposição da criança e dos danos a ela causados. Em determinado momento do episódio, um terapeuta recomenda que Marie interrompa o uso do dispositivo imediatamente para o próprio bem de Sara e comenta que o uso de *"Arkangel"* havia sido proibido na Europa (seria uma referência à GDPR?). A manutenção do uso do aparelho expõe a importância das decisões dos pais e responsáveis no que diz respeito aos melhores interesses da criança, e da própria reflexão dos limites da restrição do direito fundamental à proteção de dados na infância e adolescência.

Seja na ficção, seja no mundo real, *"Arkangel"* permite a reflexão segundo a qual, acompanhar a criança, inclusive no espaço online, é ao mesmo tempo uma necessidade e um desafio aos pais. A *hiperproteção* pode significar um prejuízo para criança nas mais diversas esferas. Nesse passo, a minimização do uso de dados e a incidência da proporcionalidade

96 Dessa maneira, "[...] as discussões apresentadas até aqui consideram fotografias e informações consideradas normais, que não extrapolam o razoável pelos conteúdos em si: são representações de filhos em situações cotidianas, que trazem aos pais autorrealização, orgulho, vontade de compartilhar com amigos e parentes etc.". SAMPAIO, Vinícius; FUJITA, Jorge Shiguemitsu. A privacidade da criança na internet: sharenting, responsabilidade parental e tratamento de dados pessoais. In: **Anais do 2º Congresso Internacional Information Society and Law – FMU – SP** – 6/11 a 8/11. 2019. p.492-493. Sobre o tema, recomenda-se também MEDON, Felipe. **Big Little Brother Brasil: pais quarentenados, filhos expostos e vigiados**. JOTA. 14 de abril de 2020. Disponível em: **https://www.jota.info/opiniao-e-analise/artigos/big-little-brother-brasil-pais-quarentenados-filhos-expostos-e-vigiados-14042020**.

97 SAMPAIO, Vinícius; FUJITA, Jorge Shiguemitsu. Obra citada, p. 492.



recomendam sempre que a dúvida oriente a não utilização dos dados, a não coleta, a destruição do dado já coletado tão logo possível.

A utilização da ferramenta de localização de filhos deve ser objeto de grande reflexão, ao poder revelar aspectos de profunda intimidade. O controle parental também precisa de controles. Neste sentido, importante ratificar que "não há uma prevalência absoluta do que os pais ou responsáveis consideram adequado ou não à criança, porque há norma anterior a essa disposição de vontade, atribuindo-lhes o dever de guarda e zelo pelos direitos do menor"[98]. Como dito, as decisões, sejam dos pais ou das empresas que atuem no tratamento de dados pessoais de crianças e adolescentes, devem ser tomadas sempre em vista do melhor interesse.

*Blackmirror* nos incita a refletir sobre as potencialidades da tecnologia, em contraste com os riscos. As ferramentas para localizar os filhos, filmá-los ou interferir no que assistem mostram-se incrivelmente factíveis e, também por isso, profundamente aterradoras.

Em um mundo em que brinquedos coletam dados, a proteção de dados deve ser tomada pelos adultos como objeto de grande atenção. A proteção da vulnerabilidade da pessoa em desenvolvimento traz consigo a necessidade de levar em conta limites que permitam assegurar o melhor interesse da criança e do adolescente, sem tolher-lhe a identidade digital que compõe, em diversas projeções, um aspecto relevante, talvez até indispensável, de sua existência em nosso atual arranjo social.

Como anuncia o título, quanto menores os titulares de dados, maiores as preocupações e desafios. A própria compreensão dos pais sobre as novas tecnologias, diante de uma *vulnerabilidade digital,* deve ser levada em conta. Ao mesmo tempo, é preciso enfrentar o tormentoso e dinâmico equilíbrio entre cuidado e controle, afeto e vigilância, infância e maturidade, autodeterminação e excesso, tecnologia e humano. Para retomar a epígrafe, tal como nas primeiras fase da vida, as perguntas a serem feitas são muitas. Quantas as implicações de todas estas transformações? Como diz Adriana Partimpim na poesia que abre o artigo, "Quanto é mil trilhões Vezes infinito?"

O percurso é longo, intenso e desafiador, e como diz Guimarães Rosa, é trilhado nas suas *grandes veredas*. Como nos adverte o escritor "Viver é etecetera".

98 SAMPAIO, Vinícius; FUJITA, Jorge Shiguemitsu. Obra citada, p.496.

# O papel das Ouvidorias Públicas na implementação da Lei Geral de Proteção de Dados (LGPD)

*Ana Lucia Lourenço*[99]

*João Daniel Vilas Boas Taques*[100]

## Introdução

Com os avanços da tecnologia e a virtualização das relações sociais e de consumo, pode-se dizer, seguramente, que o fluxo de dados e informações cresce a cada minuto. Por meio de uma simples pesquisa em um buscador, como o Google, softwares podem coletar as mais diversas informações, como a localização, deslocamento e até mesmo hábitos de consumo.

Assim, em tempos de amplo fluxo de dados e informações, potencializado pelas novas tecnologias, torna-se imperativa a regulamentação e a proteção do uso indevido dos dados pessoais compartilhados, assegurando que estes dados sejam utilizados estritamente para os fins que legitimaram sua concessão pelo titular.

Em resposta a esses novos e dinâmicos desafios, e em consonância com as políticas adotadas em escala mundial, surge a Lei Geral de Proteção de Dados (LGPD), Lei n.º 13709, sancionada em 15 de agosto de 2018.

A norma traz diversos princípios e definições, firmando, assim, os alicerces necessários para que o direito responda à essa nova e dinâmica sociedade, que, tal como as próprias tecnologias que lhe definem, está em constante mudança.

Em razão de seu caráter inovador, espera-se também que a lei traga novos desafios às pessoas físicas e jurídicas, de direito público ou privado, que operem dados, desafios

99 Bacharela em Direito pela Universidade Federal do Paraná. Desembargadora do Tribunal de Justiça do Paraná. Ouvidora de Justiça do Tribunal de Justiça do Estado do Paraná (biênio 2017/2018). Ouvidora-Geral de Justiça do Tribunal de Justiça do Estado do Paraná (biênio 2019/2020).

100 Bacharel em Direito pela Universidade Estadual de Ponta Grossa. Mestre em Direitos Humanos e Democracia pela Universidade Federal do Paraná. Pós-graduado em Direito Internacional pela Damásio Educacional.



estes que serão muito maiores ao Estado que, pela sua própria natureza e dimensão, demanda o acesso e uso de dados em uma escala muito maior.

Fruto de uma nova forma de pensamento, que preza pela participação do indivíduo, as Ouvidorias públicas podem, então, auxiliar a Administração Pública, facilitando a participação entre o ente estatal e os titulares dos dados, bem como proporcionando um maior controle social, transparência e conformidade.

Este artigo tratará, em um primeiro momento, da LGPD e suas disposições, traçando as principais linhas que orientam a norma. Em seguida, abordar-se-á as implicações da Lei na Administração Pública e seus potenciais desafios. Por fim, buscará ressaltar a importância das Ouvidorias públicas como aliadas na implementação da Lei 13.709/2018.

## Principais elementos da Lei Geral de Proteção de Dados

A Lei Geral de Proteção de Dados (LGPD) versa sobre o tratamento de dados pessoais, por pessoa natural ou por pessoa jurídica de direito público ou privado. Nos termos do seu artigo 1º, a lei tem como objetivo tutelar os direitos fundamentais de liberdade, privacidade e o personalidade.[101]

Trata-se, pois, da consolidação de um debate global que vem se desenvolvendo desde os anos 1990, quando os avanços tecnológicos, em especial o desenvolvimento da *internet*, acabou por criar um maior fluxo de dados e informações, de modo que se tornou necessário marco normativo que fizesse frente à essa nova realidade.[102]

Isso porque a geração e a captação de dados cresceram de maneira exponencial. Transações bancárias, utilização de aplicativos de transportes, publicações em redes sociais

101 **BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em 29 de agosto de 2020.**

102 Sobre o tema, leciona Pinheiro: "O motivo que inspirou o surgimento de regulamentações de proteção de dados pessoais de forma mais consistente e consolidada a partir dos anos 1990 está diretamente relacionado ao próprio desenvolvimento do modelo de negócios da economia digital, que passou a ter uma dependência muito maior dos fluxos internacionais de bases de dados, especialmente os relacionados às pessoas, viabilizados pelos avanços tecnológicos e pela globalização". PINHEIRO, Patrícia Peck. **PROTEÇÃO DE DADOS PESSOAIS: Comentários à lei nº 13.709/2018 (LGPD). São Paulo: Saraiva Educação, 2018.** *E-book. Não-paginado.*

e outros atos *online* geram grande volume de dados que, devidamente codificados, tornam-se a matéria-prima da nova economia: a informação.[103]

Esta nova economia é chamada de economia informacional, assim denominada porque a produtividade e a competividade de seus agentes dependem, essencialmente, da capacidade de trabalhar com informações nos seus mais variados níveis, da produção a aplicação. Nesse novo modelo econômico, a informação constitui elemento estruturante essencial à nova economia, do mesmo modo que o vapor e a eletricidade foram necessários às revoluções econômicas anteriores.[104]

Tem-se, nos dias de hoje, um novo modelo de negócio, baseado na monetização dos dados pessoais, em que "o pagamento – seja ele integral ou parcial – de muitos serviços é realizado com os dados pessoais do próprio consumidor"[105] [106], de modo que cabe ao Direito, à ciência jurídica, se readequar aos novos desafios emergentes desta nova realidade.

Nessa linha, a LGPD desponta como mecanismo imprescindível aos tempos atuais, ao conferir maior segurança jurídica à totalidade das operações que envolvam dados pessoais.

Compartilhando dessa posição, Pinheiro aduz que "a legislação visa fortalecer a proteção da privacidade do titular dos dados, a liberdade de expressão, de informação, de opinião e de comunicação, a inviolabilidade da intimidade, da honra e da imagem e o desenvolvimento econômico e tecnológico"[107]. Tais objetivos encontram, também, previsão expressa no artigo 2º da Lei, que estabelece as premissas fundamentais da LGPD.[108]

103 BIONI, Bruno Ricardo. **PROTEÇÃO DE DADOS PESSOAIS: a função e os limites do consentimento. Rio de Janeiro: Editora Forense, 2019.** *E-book. Não-paginado.*

104 CASTELLS, Manuel. **A Sociedade em rede. 14ª reimpressão. São Paulo: Paz e Terra, 1999. p. 114.**

105 BIONI, Bruno Ricardo. **PROTEÇÃO DE DADOS PESSOAIS: a função e os limites do consentimento. Rio de Janeiro: Editora Forense, 2019.** *E-book. Não-paginado.*

106 Sobre o tema, destaca-se também a lição de Pinheiro: "Como visto, a necessidade de uma lei específica sobre a proteção de dados pessoais decorre da forma como está sustentado o modelo atual de negócios da sociedade digital, na qual a informação passou a ser a principal moeda de troca utilizada pelos usuários para ter acesso a determinados bens, serviços ou conveniências". PINHEIRO, Patrícia Peck. **PROTEÇÃO DE DADOS PESSOAIS: Comentários à lei nº 13.709/2018 (LGPD). São Paulo: Saraiva Educação, 2018. E-book. Não-paginado.**

107 PINHEIRO, Patrícia Peck. **PROTEÇÃO DE DADOS PESSOAIS: Comentários à lei nº 13.709/2018 (LGPD). São Paulo: Saraiva Educação, 2018. E-book. Não-paginado.**

108 **BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em 29 de agosto de 2020.**



Trata-se, também, de uma legislação principiológica[109],na medida em que estabelece amplo rol de princípios que, em razão da sua importância à privacidade do titular e dos seus dados[110], devem ser observados. São eles:

> *Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:*
>
> *I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;*
>
> *II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;*
>
> *III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;*
>
> *IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;*
>
> *V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;*
>
> *VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;*
>
> *VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;*

109 PINHEIRO, Patrícia Peck. **PROTEÇÃO DE DADOS PESSOAIS: Comentários à lei nº 13.709/2018 (LGPD). São Paulo: Saraiva Educação, 2018. E-book. Não-paginado.**

110 "É uma carga principiológica que procura conformar, justamente, a ideia de que o titular dos dados pessoais deve ser empoderado com o controle de suas informações pessoais e, sobretudo, na sua autonomia da vontade". BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento. Rio de Janeiro: Editora Forense, 2019.** *E-book. Não paginado.*

*VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;*

*IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;*

*X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.*

Os princípios adotados resultam da convergência dos objetivos e linhas de atuação presentes nas mais diversas leis estrangeiras que tratam sobre a proteção de dados, vinculando a norma, ainda, à proteção da dignidade da pessoa humana e seus direitos fundamentais.[111]

Devido ao seu caráter inovador, o marco normativo em análise também traz a definição de alguns conceitos e terminologias essenciais às operações envolvendo dados, que encontram previsão em seu artigo 5º. Aliás, a própria operação de dados recebe o nome de "tratamento" (art. 5º, X), sendo definido como toda operação realizada com dados pessoais, aí inclusas a coleta, produção, utilização, acesso, reprodução, processamento e qualquer outra atividade realizada sobre os dados.[112]

Nos termos do artigo 5º, I, dado pessoal é toda a informação relacionada a pessoa natural identificada ou identificável. Os dados também podem ser definidos como "sensíveis", o que ocorre quando relacionados às características da personalidade do indivíduo ou escolhas pessoais.[113] Apresentam esta característica distintiva em razão do seu conteúdo oferecer um maior vulnerabilidade, dado que sujeito a atos discriminatórios.

A lei também define como "titular" a pessoa natural, cujos dados pessoais são objeto de tratamento. O titular dos dados pessoais tem papel privilegiado nas operações, sendo-

111 DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico Journal of Law [EJJL], 2011, 12(2), 91-108. p. 98.**

112 **BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em 29 de agosto de 2020.**

113 PINHEIRO, Patrícia Peck. **Proteção de Dados Pessoais: Comentários à lei nº 13.709/2018 (LGPD). São Paulo: Saraiva Educação, 2018. E-book. Não-paginado.**



-lhe outorgado o direito à autodeterminação informativa, cujos efeitos irradiam ao longo de toda a redação normativa.

Com previsão artigo 2º, II, da LGPD, a consagração da autodeterminação informativa é um dos principais pontos a serem destacados na lei.

Trata-se de uma evolução, e também alargamento, do direito à intimidade, definido em sua tradicional matriz liberal como o "direito de estar só", ainda em 1890, que buscava tutelar a vida íntima, familiar e pessoal do indivíduo[114]. Contudo, na redefinida análise contemporânea, este direito passou a ser entendido, ante o advento da modernidade e a alteração das relações sociais, como o direito a controlar, endereçar e até mesmo interromper os próprios dados e informações.[115]

Tal princípio surgiu no Tribunal Federal Constitucional Alemão, ao julgar uma legislação censitária em 1983, que reconheceu a possibilidade de uma autodeterminação informativa, sob o argumento de que a proteção do indivíduo contra a coleta, armazenamento, uso e divulgação de seus dados derivaria dos direitos da personalidade. A única limitação a esse direito se daria nos casos de interesse público.[116]

Surge, assim, a privacidade enquanto autodeterminação informativa, que possibilita ao indivíduo o controle sobre o fluxo de suas informações. Para Doneda, a autodeterminação informativa se traduz no direito do indivíduo de controlar a obtenção, titularidade, tratamento e transmissão dos seus dados pessoais.[117]

A autodeterminação informativa é o fundamento sobre o qual se erige a LGPD, na medida em que trata de uma manifestação direta dos direitos constitucionais da intimidade, privacidade e personalidade. É com base neste direito que o indivíduo assume o papel de protagonista no tratamento de seus dados.

114 WARREN, Samuel D. BRANDEIS, Louis D. The right to privacy. p. 193-220. **Harvard Law Review, Vol. 4, No. 5. (Dec. 15, 1890).**

115 RODOTÀ, Stefano. **A vida na sociedade de vigilância. Rio de Janeiro: Renovar, 2008. p. 92.**

116 CACHAPUZ, Maria Cláudia Mércio. Privacidade, proteção de dados e autodeterminação informativa. p. 823-848. **Revista Jurídica da Presidência. Brasília v. 15 n. 107 Out. 2013/Jan. 2014. p. 827.**

117 DONEDA, Danilo. A Proteção dos Dados Pessoais como um Direito Fundamental. **Espaço Jurídico. Joaçaba, v. 12, n. 2, p. 91-108, jul./dez. 2011. Disponível em: https://portalperiodicos.unoesc.edu.br/ espacojuridico/article/view/1315/658. Acesso em: 29 de agosto de 2020.**

Por esse princípio, o titular deixa de ser apenas mero fornecedor de dados, assumindo um papel ativo e de destaque, em que tem o direito de acompanhar todo o processo de tratamento dos dados, da coleta ao seu termo, o que justifica a extensa previsão de direitos que lhe são atribuídos ao longo da lei, efetivando a premissa de participação ativa na gestão de dados.

A partir da ideia de que os dados e informações constituem exteriorização do indivíduo, a autodeterminação informativa assume papel essencial à salvaguarda da liberdade, privacidade e desenvolvimento da pessoa natural, direitos estes previstos no artigo 1º da LGPD e também na Constituição Federal. O titular passa a interagir e intervir no processo de tratamento de dados.

A autodeterminação informativa tem fundamento, pois, no consentimento do indivíduo, condição necessária ao tratamento de dados, somente dispensável nas hipóteses previstas no artigo 7º (cumprimento de obrigação legal, execução de políticas públicas, pesquisas, proteção de crédito e outras).

Em face da vulnerabilidade que advém da circulação dos dados pessoais, potencializada pela internet, torna-se necessária a manifestação clara do titular para garantir que tem conhecimento de que seus dados serão captados e utilizados, bem como a finalidade para a qual serão destinados.

O consentimento é a exteriorização da própria autodeterminação informativa. É o que define o sentido e o alcance da autodeterminação informativa, vinculando todos os envolvidos no tratamento de dados à livre vontade do titular.[118] Modificada a finalidade do tratamento dos dados, por exemplo, faz-se necessário novo consentimento do titular.

A LGPD estabelece que o consentimento deve ser praticado pela pessoa natural titular dos dados, ou por seu responsável legal, e deve demonstrar, ainda, a livre manifestação de vontade do indivíduo, que deve ser livre, informada, inequívoca e determinada.

118 SILVA, Paulo Henrique Tavares da. SOUSA, Rosilene Paiva Marinho de. PROTEÇÃO DE DADOS PESSOAIS E OS CONTORNOS DA AUTODETERMINAÇÃO INFORMATIVA. **Inf. & Soc.:Est., João Pessoa, v.30, n.2, p. 1-19, abr./jun. 2020. p. 11.**



O consentimento livre é a escolha que o indivíduo tem de optar pela aceitação ou recusa de compartilhamento de seus dados, sem que isto lhe cause qualquer prejuízo. O indivíduo pode decidir, inclusive, quais os dados serão fornecidos e quando serão revogados. Contudo, a liberdade de escolha pode sofrer limitações, como nos casos de serviços que somente serão fornecidos se houver a troca de informações.[119]

Deve-se entender que as entidades responsáveis pelo tratamento de dados devem fornecer todas as possibilidades de utilização dos dados ao usuário, enquanto que por inequívoco se tem que o usuário deve consentir de forma ativa. O consentimento deve ser, também, determinado, devendo ser informado ao usuário a extensão do tratamento, os agentes envolvidos e as condições específicas.[120]

O art. 9º, § 1º, estabelece que o consentimento será considerado nulo se o titular tiver sido exposto a conteúdo enganoso ou abusivo, ou se não tiver sido demonstrado de forma clara e inequívoca o modo de tratamento dos dados. Do mesmo modo, será considerado nulo o consentimento que seja formulado de forma genérica.

Para que o Consentimento seja considerado válido, é necessária a observância dos elementos previstos em sua própria definição (art. 5º, XII), segundo a qual o consentimento deve ser livre, informado e inequívoco e com uma finalidade determinada. Em se tratando de dados sensíveis, o consentimento deve ser, ainda, fornecido de forma específica e destaca, consoante dispõe o artigo 11, I, da LGPD.

Em observância ao disposto na lei, o consentimento não se encerra no momento na simples permissão para a coleta dos dados, tornando-se a linha mestra pelo qual a operação se desenvolve, vinculando todo o processo de tratamento dos dados à vontade do agente, como a utilização, processamento, transmissão, compartilhamento e qualquer outra atividade.

119 MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014. p. 41.**

120 FRAZÃO, Ana; OLIVA, Milena Donato; TEPEDINO, Gustavo. **Lei Geral de Proteção de Dados Pessoais e Suas Repercussões no Direito Brasileiro. São Paulo: Revista dos Tribunais, 2019. p. 299-302.**

O titular dos dados pessoais assume, assim, o protagonismo nas relações de operação de dados pessoais, sendo parte essencial não apenas à coleta, mas também na destinação dos dados, cabendo ao operador dos dados observar os limites impostos.

Um outro direito importante na LGPD está o que confere ao titular a possibilidade de acessar, corrigir, anonimizar e até mesmo eliminar dados, nos termos do artigo 18 da Lei. Sobre o tema, a lição de Frazão *et al.*:

> *Por conseguinte, revela-se impossível cogitar de proteção integral à liberdade, à privacidade e ao desenvolvimento da pessoa natural sem que se lhe garanta eficaz defesa e controle de seus próprios dados – o que se traduz na expressão autodeterminação informativa.*
>
> *[...]*
>
> *Daí a expressa referência do legislador brasileiro de que a proteção conferida tem o objetivo de "proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural" (art. 1º), verdadeira premissa que deve orientar a interpretação de todos os preceitos da LGPD.*[121]

A anonimização esta definida como a técnica que retira do dado a capacidade de associação, direta ou indireta, a um indivíduo, quebrando o vínculo entre o titular e o dado.[122]

O processo de anonimização busca eliminar os chamados "elementos identificadores" em uma base de dados, podendo se dar por meio de supressão, generalização, randomização e pseudoanonimização.[123]

A anonimização não se limita, pois, aos identificadores diretos, como nome e documentos, abrangendo, também, os dados como *internet protocol* (IP) e *cookies*, que podem ser utilizados, por exemplo, para definir os padrões de consumo do usuário.

121 FRAZÃO, Ana; OLIVA, Milena Donato e; ABILIO, Vivianne da Silveira. Compliance de dados pessoais (p. 677-715). In FRAZÃO, Ana. TEPEDINO, Gustavo e; OLIVA, Milena Donato. **A lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro. São Paulo: Thomson Reuters, 2019. 678.**

122 DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006. p. 44.

123 BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. Rio de Janeiro: Editora Forense, 2019. E-book. Não paginado.



A LGPD, tal como seu equivalente europeu, adotou um conceito reducionista de anonimização, que admite que toda anonimização de dado é passível de falhas, podendo se tornar, novamente, identificável, refutando, assim, a suposição de anonimização robusta[124].

Para tanto, a LGPD se valeu do que Bioni define como "critério da razoabilidade", segundo o qual se exige, quando da anonimização, a utilização dos meios técnicos razoáveis e disponíveis no momento.[125] Assim, por essa lógica, se foi necessário um esforço além do razoável para a identificação do titular por meio de determinado dado, resulta descaracterizada a relação técnica de dado pessoal.

A lei define, também, os agentes de tratamento, ou seja, aqueles responsáveis pela coleta e instrumentalização das informações fornecidas pelo titular. São eles: o controlador, o operador e o encarregado.[126]

Os agentes são obrigados a manter registro das operações de tratamento que realizaram (art. 37), apontando neste a finalidade, tempo de processamento, prazo e sigilo, bem como as hipóteses em que houver exclusão de consentimento. Trata-se, pois, do aspecto preventivo da lei, que tem como objetivo conferir maior proteção ao titular. Nesse sentido, Frazão *et al*. entendem que a normativa possui contundente aspecto preventivo, com o objetivo de evitar qualquer prejuízo ao titular de dados.[127]

O controlador é o principal responsável pelo tratamento dos dados, enquanto que o operador, por sua vez, é mandatário, operando os dados pessoais conforme lhe for instruído (art. 39). Sobre eles recai a responsabilidade pelo correto tratamento dos dados. Nos termos do artigo 42 da norma, se, em razão do exercício de atividade de tratamento de

124 DONEDA, Danilo. MACHADO, Diego. Proteção de dados pessoais e criptografia: tecnologias criptográficas entre anonimização e psudonimização de dados. p. 99-128. Revista dos Tribunais. vol. 998. São Paulo: Editora Revista dos Tribunais, 2018. p. 110.

125 BIONI, Bruno. Compreendendo o conceito de anonimização e dado anonimizado. p. 191-201. **Cadernos Jurídicos. São Paulo, ano 21, nº 53. Janeiro-Março/2020. p. 192.**

126 **BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em 29 de agosto de 2020.**

127 FRAZÃO, Ana; OLIVA, Milena Donato e; ABILIO, Vivianne da Silveira. Compliance de dados pessoais (p. 677-715). In FRAZÃO, Ana. TEPEDINO, Gustavo e; OLIVA, Milena Donato. **A lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro. São Paulo: Thomson Reuters, 2019. 681.**

dados pessoais e em violação à LGPD, causarem dano patrimonial, moral, individual ou coletivo, serão obrigados a repará-lo.

A responsabilização será afastada em três hipóteses: quando ficar provado que os agentes não realizaram o tratamento; quando, embora tenham realizado o tratamento, não houver qualquer violação às disposições da LGPD; e quando a culpa pelo dano for exclusivamente do titular dos dados ou terceiro estranho ao tratamento.

Por meio da responsabilização dos agentes, busca-se preservar a autodeterminação informativa do titular. Trata-se, pois, de garantia de proteção aos direitos assegurados na lei, que, como dito alhures, assumem uma nova importância no atual modelo econômico.

Outro agente importante é o "encarregado", com inspiração no Data Protection Officer (DPO) da GDPR europeia. O agente é definido como pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados.

Nos termos do artigo 41, § 2º, as atividades do encarregado consistem em aceitar reclamações e comunicações dos titulares e da autoridade nacional, prestar esclarecimentos e adotar providências, bem como orientar os funcionários da entidade a respeito das práticas a serem tomadas em relação à proteção de dados.

O papel de encarregado se mostra de vital importância à implementação da proteção de dados, pois se trata de peça chave ao exercício da autodeterminação informativa, estabelecendo o essencial contato entre o titular e os operadores dos dados. Permite-se, assim, por meio do encarregado, que o titular formule requerimentos e requisite informações sobre o tratamento de dados realizado.

Tem-se, assim, uma lei ampla em princípios e terminologias que busca dar prioridade ao titular, que, com o controle de seus dados, exercita a autodeterminação informativa.

## A LGPD e a Administração Pública

Em se tratando de coleta, armazenamento e manipulação de dados a Administração Pública assume papel de destaque. Isso porque a sua atuação, pela sua própria natureza, demanda o amplo acesso e o uso de dados (pessoais ou não) – de modo a permitir, facilitar e conferir maior eficiência a atividade administrativa.[128]

Tome-se o Estado brasileiro, por exemplo. Por meio dos inúmeros documentos oficiais, declarações de renda, movimentos bancários e cadastro previdenciário, evidencia-se que a Administração dispõe de ampla gama de dados e informações. Neste sentido, Scopel entende que o Poder Público maneja, inclusive, uma ampla gama de dados sensíveis, como os de origem racial e referentes à saúde, como os prontuários médicos guardados pelo Sistema Único de Saúde.[129]

Em razão desse volume, a Administração também está sujeita à maiores riscos, bem como a um maior potencial de dano aos titulares. Em 2015, por exemplo, 191 milhões de estadunidenses tiveram seus dados pessoais violados. Os dados envolviam nome, endereço, data de nascimento, afiliações partidárias, números de telefone e e-mails, afetando os 50 estados e o distrito federal.[130] Na Índia, o vazamento dos dados contidos na base de dados Aadhar, a maior do mundo, atingiu mais de 1 bilhão de pessoas. Os dados, neste caso, envolviam, inclusive, informação biométrica, que poderia ser utilizada para abrir contas bancárias.[131]

É necessário atentar ainda para os riscos decorrentes do Estado de vigilância, que, tal como na fábula orwelliana "1984"[132], se reveste de caráter autoritário. Os altos índices de violência no Brasil, bem como a insegurança generalizada por parte da população,

128 SCOPEL, Adriano Sayão. Breves considerações sobre tratamento de dados pelo Poder Público e meios de defesa dos dados pessoais por particulares. **Revista de Direito e as Novas Tecnologias | vol. 7/2020 | Abr - Jun / 2020.**

129 SCOPEL, Adriano Sayão. Breves considerações sobre tratamento de dados pelo Poder Público e meios de defesa dos dados pessoais por particulares. **Revista de Direito e as Novas Tecnologias | vol. 7/2020 | Abr - Jun / 2020.**

130 FINKLE, Jim; VOLZ, Dustin. Database of 191 million U.S. voters exposed on Internet: researcher. **Reuters. Publicado em 28 de dezembro de 2015. Disponível em < https://uk.reuters.com/article/us-usa-voters-breach-idUKKBN0UB1E020151229>. Acesso em 30 de agosto de 2020.**

131 Aadhar: 'Leak' in world's biggest database worries Indians. **BBC News. Publicado em 05 de janeiro de 2018. Disponível em < https://www.bbc.com/news/world-asia-india-42575443>. Acesso em 30 de agosto de 2020.**

132 ORWELL, George. **1984. 1ª ed. São Paulo: Companhia das Letras. 2009. Tradução de Alexandre Hubner e Heloisa Jahn.**

constituem ambiente propício ao afrouxamento dos limites impostos à coleta de dados, o que, por sua vez, pode levar a arroubos autoritários por parte do Estado.[133]

A LGPD deixou inequívoca, já em seu artigo 1º, a sua incidência sobre os órgãos públicos ("ou por pessoa jurídica de direito público"). Ademais, além das previsões gerais dispostas no texto, que se aplicam às pessoas naturais ou jurídicas de direito público ou privado, a Lei também destinou um capítulo específico ao tratamento de dados pessoais pelo poder público, no caso os artigos 23 a 32.

Sucede que, diante da promulgação da Lei 13.709/2018, surgem algumas controvérsias a respeito da aplicação de alguns dos dispositivos da referida lei ao Poder Público. Dentre os pontos controversos, acentua-se a obrigatoriedade de consentimento do titular, consoante dispõe o art. 26 da LGPD. A respeito desse tema, Adami *et al*. afirmam que, por vezes, o cidadão não possui uma liberdade de escolha em relação a coleta de dados, pois o seu tratamento é essencial às atividades desenvolvidas pelo Poder Público.[134] Cita-se, como exemplo, a ampla gama de informações coletada pela Justiça Eleitoral, como endereço e dados biométricos, mas que são essenciais à manutenção da democracia.

O artigo 23, em observância ao disposto no Lei de Acesso à Informação, indica quais pessoas jurídicas estão efetivamente sujeitas às normas da LGPD: os órgãos públicos integrantes da Administração direta dos Poderes Executivo, Legislativo, incluindo as Cortes de Contas, Poder Judiciário e do Ministério Público, e as autarquias, as fundações públicas, as empresas públicas, as sociedades de economia mista e demais entidades controladas direta ou indiretamente pela União, Estados, Distrito Federal e Municípios. Também devem ser somados à lista os serviços notariais e de registro, exercidos em caráter privado, por delegação do Poder Público (art. 23, § 4º).

133 CORRÊA, Adriana Espíndola. Lei de proteção de dados e identificação nacional: há antinomias? **Revista Síntese Direito Civil e Processual Civil, Porto Alegre, v.19, n.120, p. 9-16, jul./ago. 2019.**

134 ADAMI, Mateus Piva. DOUEK, Daniel. FARIAS, Pedro. LANGENEGGER, Natalia. PARISIO, Isabela de Oliveira. Tratamento de dados pessoais pela administração pública: análise do SERPRO. p. 193-224. In **Proteção de dados pessoais no Brasil: uma nova visão a partir da Lei nº 13.709/2018 (coord. Paulo Marcos Rodrigues Brancher e Anna Claudia Beppu). Belo Horizonte: Fórum, 2019.**



O dispositivo em comento estabelece, ainda, que o tratamento dos dados pessoais deve atender a sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público[135], observando-se, ainda, duas condições:

> *Incumbe ao Poder Público informar – o texto legal não diz a quem, mas infere-se que seja aos titulares dos dados – o fundamento legal e a finalidade da coleta e tratamento dos dados pessoais coletados, bem como indicar quem será o encarregado (pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a agência nacional de proteção de dados). Logo, conclui-se que o Poder Público não pode exigir todo e qualquer dado pessoal do particular, mas somente o que seja necessário para suas atividades públicas.*[136]

Tem-se, assim, que a exigência do Poder Público de dados e informações pessoais deve estar limitada somente ao essencial para seus propósitos.

O poder público pode também compartilhar dados (art. 26, *caput*), desde que observadas as finalidades específicas de execução de políticas, bem como os princípios previstos no artigo 6º da Lei. O Poder Público tem o dever de garantir que o compartilhamento de dados observe os princípios e dispositivos elencados na LGPD.[137]

Contudo, é vedado à administração pública transferir informações a entidades privadas, exceto em casos de execução descentralizada de atividade pública, em que os dados forem de acesso público, quando houver previsão legal para tanto, quando respaldada em contratos e convênios e, por fim, quando a transferência objetivar a prevenção de fraudes e irregularidades (art. 26, § 1º).

135 "Da mesma forma que as instituições privadas devem apresentar uma finalidade clara e transparente para a realização do tratamento de dados pessoais, a pessoa jurídica de direito público deve adotar a finalidade pública e o interesse público para a realização de tratamento de dados". PINHEIRO, Patricia Peck. PINHEIRO, Patrícia Peck. **Proteção de Dados Pessoais: Comentários à lei nº 13.709/2018 (LGPD). São Paulo: Saraiva Educação, 2018. E-book. Não-paginado.**

136 SCOPEL, Adriano Sayão. Breves considerações sobre tratamento de dados pelo Poder Público e meios de defesa dos dados pessoais por particulares. **Revista de Direito e as Novas Tecnologias | vol. 7/2020 | Abr - Jun / 2020.**

137 PINHEIRO, Patricia Peck. PINHEIRO, Patrícia Peck. **Proteção de Dados Pessoais: Comentários à lei nº 13.709/2018 (LGPD). São Paulo: Saraiva Educação, 2018. E-book. Não-paginado.**

Além da já visitada regra geral de responsabilidade prevista no artigo 42, a LGPD também trouxe regras específicas de responsabilidade destinadas ao Poder Público, em harmonia ao disposto no artigo 37, § 6º, da Constituição Federal. Os artigos 31 e 32 da Lei estabelecem que quando houver infração aos dispositivos legais pelos órgãos públicos, a Autoridade Nacional de Proteção de Dados (ANPD) poderá enviar informe com as medidas necessários a correção da violação, bem como solicitar aos agentes a publicação de relatórios. Scopel critica tais dispositivos afirmando que se trata, pois, de uma "tímida e inócua previsão de possibilidades", que sequer são obrigatórias.[138]

Assim, do ponto de vista do direito público, tem-se que, em razão da sua amplitude, os órgãos da administração estão sujeitos a um rigor maior do que o imposto as entidades privadas, representando novo desafio a ser superado pela administração.

## O papel das Ouvidorias públicas na implementação da LGPD

Para que exista, de fato, um controle social, em pleno funcionamento, faz-se necessário que o titular e a sociedade civil participem ativamente do controle e operação de dados. Em face dos novos desafios trazidos pela LGPD, as ouvidorias públicas surgem como uma aliada, proporcionando espaço seguro para o diálogo e controle entre a Administração e o titular dos dados.

As ouvidorias públicas possuem origem na Suécia, entre os séculos XVIII e XIX, quando surgiu a figura do *ombudsman*. A tradução literal do termo *ombudsman* para o português é "mediador", aquele que mediava a comunicação entre os cidadãos e o Poder Público.[139]

As ouvidorias públicas estão essencialmente ligadas à participação da população na gestão da administração pública, pois são um instrumento essencial ao efetivo e direto

138 SCOPEL, Adriano Sayão. Breves considerações sobre tratamento de dados pelo Poder Público e meios de defesa dos dados pessoais por particulares. **Revista de Direito e as Novas Tecnologias | vol. 7/2020 | Abr - Jun / 2020.**

139 CARDOSO, Antonio Semeraro Rito. ÂLCANTARA, Elton Luiz da Costa. e LIMA NETO, Fernando Cardoso. Ouvidoria pública e governança democrática. In **Transparência e Controle Social: Revista do Tribunal de Contas do Estado de Minas Gerais. Ano 1, n. 1 (dez. 1983- ). Belo Horizonte: Tribunal de Contas do Estado de Minas Gerais, 1983. P. 29-40. p. 29.**



controle social das instituições por parte da sociedade civil. Neste sentido, leciona Cardoso que o controle social exige um inclusão social, que se dá por meio de participação ativa da sociedade na gestão pública, que permite ao cidadão sair do papel de mero destinatário da atividade estatal e participar da administração pública, de acordo com a construção do bem comum.[140]

Na condição de facilitadoras do diálogo, as ouvidorias podem e devem assumir papel de destaque na implementação e efetivação da LGPD.

Uma das possibilidades é a de as ouvidorias assumam o papel de encarregado, previsto no artigo 41 da Lei.

A atuação prevista no artigo 41 da LGPD já encontrava previsão semelhante no artigo 40 da Lei de Acesso à Informação (LAI), que prescrevia a designação de autoridade para efetivar o monitoramento e *compliance* da administração pública com a disposição previstas na referida lei.

Em pesquisa realizada pela Controladoria-Geral da União (CGU) e pela Unesco, verificou-se a possibilidade de as ouvidorias assumirem as responsabilidades previstas no artigo 40 da LAI. Isso se daria em razão do fato de tanto a autoridade do artigo 40 quanto as ouvidorias apresentarem responsabilidades congêneres, não apenas para garantir o acesso do indivíduo à administração pública, mas também para auxiliar na governança institucional.

Nessa linha, tem-se, portanto, a possibilidade de as ouvidorias também assumirem a função de encarregado, semelhante ao papel já desempenhado em observância ao artigo 40 da LAI.

Inspirado na figura do DPO da sistemática europeia, o artigo 5º, VIII, da LGPD define "encarregado" como a "pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD)". Dispõe também o artigo 41 que o encarregado será

140 CARDOSO, Antonio Semeraro Rito. Ouvidoria pública como instrumento de mudança. **Instituto de Pesquisa Econômica Aplicada (IPEA): Brasília, 2010. p. 13.**

responsável pela comunicação entre o ente responsável pelo tratamento de dados, o titular e a ANPD. É o responsável, ainda, pela governança institucional, auxiliando na implementação de ações que reforcem a LGPD.[141] Sobre o tema, Hang e Kaunert afirmam o seguinte:

> *Esse canal de comunicação estabelecido entre os envolvidos no tratamento de dados é de vital importância, porque define e centraliza na pessoa do encarregado as informações das providências tomadas ou que devam ser tomadas, ou seja, é ele quem deve ser procurado para todos os esclarecimentos e requerimentos que dizem respeito ao tratamento de dados. Daí a importância da documentação e registro de todos os atos.*[142]

Trata-se, pois, de figura essencial à LGPD; por meio de suas funções de informação, controle e aconselhamento, o encarregado pode impulsionar e harmonizar as operações de dados em sua instituição.

Ao atuar como canal de comunicação entre os agentes, titulares e órgãos competentes, pode-se afirmar que o papel das ouvidorias e do encarregado possuem similaridade dando margem, portanto, à possibilidade de se concentrar em uma única figura. Isso porque ambos possuem a obrigação de facilitar a participação, o controle social, a transparência e a conformidade, dando o devido encaminhamento às manifestações do titular para que sejam prestados esclarecimento, garantindo, assim, o exercício de direitos de acesso, retificação, portabilidade dos dados.

Por meio da análise das requisições, o encarregado pode orientar a entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais. Concentrando-se esta função nas ouvidorias, as políticas de proteção de dados terão maior alcance na instituição, inserindo-se nas práticas de governança.

141 **BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em 30 de agosto de 2020.**

142 HANG, Cristina. Kaunert, Jane. Dos agentes de tratamento de dados. p. 88-106. In **Comentários à Lei Geral de Proteção de Dados. (Coord. Regiane Martines dos Santos e Adriana Cristina F. L. de Carvalho. Comissão de Direito Digital, Tecnologia e Inteligência Artificial. OAB-SP 116ª Subsecção. Jabaquara. 2020. p. 97.**



A governança pública associa-se a um movimento capitaneado pelo Banco Mundial no final do século XX, que buscava melhorar a prestação dos serviços públicos à população, por meio, principalmente, de um maior envolvimento da sociedade civil.

Na condição de instrumentos de participação direta, as ouvidorias podem e devem assumir papel de liderança nas práticas de governança de proteção de dados, potencializando a participação do titular, e também da sociedade, no Poder Público.

Sob esta ótica, as ouvidorias têm o condão de realizar e promover estudos, implementar projetos, fazer diagnósticos e promover a capacitação dos servidores, o que se mostra essencial na implementação dessa nova cultura voltada à proteção de dados do titular, direcionando e, se necessário, reposicionado a atuação e prestação de serviços da Administração Pública.

As ouvidorias podem, também, assumir papel auxiliar na implementação da LGPD. Isso porque, por serem uma figura externa e prévia às normas de proteção de dados, criadas anteriormente à LGPD, bem como por terem uma atuação que vai além do tratamento de dados, elas mesmas podem ser objeto de controle e até mesmo censura nos termos da Lei.

Tratar-se-ia, pois, de um arranjo descentralizado, em que a ouvidoria e os agentes da LGPD estão distribuídos por diversas pessoas. Essa organização descentralizada já foi adotada quando da implementação da LAI, em que alguns órgãos como o Ministério da Fazenda e o Banco Central do Brasil separaram a autoridade prevista no artigo 40 da Lei 12.527/2011 e as ouvidorias.[143]

A arquitetura organizacional descentralizada tem como vantagens a promoção da neutralidade e imparcialidade, evitando-se a confusão de interesses entre as ouvidorias e o tratamento de dados, que pode acabar por gerar uma interpretação diversa.

Assim, o encarregado seria uma figura criada especificamente nos termos da LGPD e para as funções ali previstas, enquanto às ouvidorias seria destinado o papel de auxiliar na implementação e integração da proteção de dados às instituições.

143 Controladoria-Geral da União. Orientações para a implementação da Lei de Acesso à Informação nas Ouvidorias Públicas: rumo ao sistema participativo. **Coleção OGU. Brasília, 2012.**

As ouvidorias públicas já representam uma nova cultura que objetiva maior participação do indivíduo na administração, colocando-o no centro do debate sobre a organização estatal. Essa cultura se originou já na redemocratização, na medida em que a Constituição Federal trouxe novo contexto social, de revitalização da cidadania, em que o controle social e o envolvimento da sociedade civil são elementares à própria essência do Estado brasileiro.

Do mesmo modo, a LGPD se insere nessa dinâmica, por meio da consagração da autodeterminação informativa, tendo como ponto principal a participação do indivíduo no tratamento de dados pessoais. Na lição de Santos e Taliba, consagrou-se um regime de participação entre titular de dados e os agentes, em que deve observar os interesses do primeiro.[144]

Assim, por terem origem semelhante na participação do indivíduo, as ouvidorias podem auxiliar o debate em prol de uma mudança cultural que estabeleça a ideia de que os dados pessoais são merecedores de proteção jurídica.

## Conclusão

Em face do avanço das tecnologias, a virtualização das relações, o crescente fluxo de dados pessoais e a sua monetização, a proteção de dados se tornou essencial à proteção não apenas do cidadão, mas também da sociedade como um todo, que vê a privacidade desaparecer em um mundo cada vez mais conectado.

Impõe-se, assim, a operação responsável dos dados pessoais dos cidadãos, para que lhe seja proporcionada a segurança necessária a participação em um mundo cada vez mais conectado, sem abrir mão do direito fundamental à privacidade.

Frente aos novos e dinâmicos desafios da atualidade, as ouvidorias públicas, por meio de reclamações, sugestões, críticas e elogios, possuem o potencial de auxiliar a administração pública na implementação da Lei Geral de Proteção de Dados, viabilizando canal de interação entre o cidadão e a administração pública.

144 SANTOS, Fabíola Meira de Almeida; TALIBA, Rita. Lei Geral de Proteção de Dados no Brasil e os possíveis impactos. **Revista dos Tribunais | vol. 998/2018 | p. 225 - 239 | Dez / 2018. Não-paginado.**



Isso decorre, em grande medida, do fato de ambos os institutos estarem ligados a uma nova forma de gestão participativa, que pressupõe maior destaque do indivíduo na esfera da administração pública, no caso da proteção de dados, por meio da autodeterminação informativa recém consagrada, ou como cidadão, responsável pelo controle social das instituições.

Afinal, se a sociedade da informação se baseia em conexões e fluxos, os mecanismos de controle e proteção também devem operar nas mesmas bases, criando-se, assim, uma verdadeira rede de comunicação entre o indivíduo, detentor dos dados, e os operadores, em última análise, entre a sociedade e o Estado.

## Bibliografia


ADAMI, Mateus Piva. DOUEK, Daniel. FARIAS, Pedro. LANGENEGGER, Natalia. PARISIO, Isabela de Oliveira. Tratamento de dados pessoais pela administração pública: análise do SERPRO. p. 193-224. In **Proteção de dados pessoais no Brasil**: uma nova visão a partir da Lei nº 13.709/2018 (coord. Paulo Marcos Rodrigues Brancher e Anna Claudia Beppu). Belo Horizonte: Fórum, 2019.

**BRASIL**. Lei nº 13.709, de 14 de agosto de 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em 29 de agosto de 2020.

BIONI, Bruno Ricardo. **PROTEÇÃO DE DADOS PESSOAIS**: a função e os limites do consentimento. Rio de Janeiro: Editora Forense, 2019. *E-book*.

BIONI, Bruno. Compreendendo o conceito de anonimização e dado anonimizado. p. 191-201. **Cadernos Jurídicos**. São Paulo, ano 21, nº 53. Janeiro-Março/2020.

CARDOSO, Antonio Semeraro Rito. Ouvidoria pública como instrumento de mudança. **Instituto de Pesquisa Econômica Aplicada** (IPEA): Brasília, 2010.

CARDOSO, Antonio Semeraro Rito. ÂLCANTARA, Elton Luiz da Costa. e LIMA NETO, Fernando Cardoso. Ouvidoria pública e governança democrática. In **Transparência e Controle Social**: Revista do Tribunal de Contas do Estado de Minas Gerais. Ano 1, n. 1 (dez. 1983- ). Belo Horizonte: Tribunal de Contas do Estado de Minas Gerais, 1983.

CASTELLS, Manuel. **A Sociedade em rede**. 14ª reimpressão. São Paulo: Paz e Terra, 1999.

Controladoria-Geral da União. Orientações para a implementação da Lei de Acesso à Informação nas Ouvidorias Públicas: rumo ao sistema participativo. **Coleção OGU**. Brasília, 2012.

CORRÊA, Adriana Espíndola. Lei de proteção de dados e identificação nacional: há antinomias?. In **Revista Síntese Direito Civil e Processual Civil**, Porto Alegre, v.19, n.120, p. 9-16, jul./ago. 2019.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico Journal of Law** [EJJL], 2011, 12(2), 91-108.

DONEDA, Danilo. A Proteção dos Dados Pessoais como um Direito Fundamental. **Espaço Jurídico**. Joaçaba, v. 12, n. 2, p. 91-108, jul./dez. 2011. Disponível em: https://portalperiodicos.unoesc.edu.br/ espacojuridico/article/view/1315/658.

DONEDA, Danilo. MACHADO, Diego. Proteção de dados pessoais e criptografia: tecnologias criptográficas entre anonimização e psudonimização de dados. p. 99-128. **Revista dos Tribunais**. vol. 998. São Paulo: Editora Revista dos Tribunais, 2018.

FINKLE, Jim; VOLZ, Dustin. Database of 191 million U.S. voters exposed on Internet: researcher. **Reuters**. Publicado em 28 de dezembro de 2015. Disponível em < https://uk.reuters.com/article/us-usa-voters-breach-idUKKBN0UB1E020151229>. Acesso em 30 de agosto de 2020.

FRAZÃO, Ana; OLIVA, Milena Donato e; ABILIO, Vivianne da Silveira. Compliance de dados pessoais (p. 677-715). In FRAZÃO, Ana. TEPEDINO, Gustavo e; OLIVA, Milena Donato. **A lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro**. São Paulo: Thomson Reuters, 2019.

FRAZÃO, Ana; OLIVA, Milena Donato; TEPEDINO, Gustavo. **Lei Geral de Proteção de Dados Pessoais e Suas Repercussões no Direito Brasileiro**. São Paulo: Revista dos Tribunais, 2019.



HANG, Cristina. Kaunert, Jane. Dos agentes de tratamento de dados. p. 88-106. In **Comentários à Lei Geral de Proteção de Dados**. (Coord. Regiane Martines dos Santos e Adriana Cristina F. L. de Carvalho. Comissão de Direito Digital, Tecnologia e Inteligência Artificial. OAB-SP 116ª Subsecção. Jabaquara. 2020.

MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.

ORWELL, George. **1984**. 1ª ed. São Paulo: Companhia das Letras. 2009. Tradução de Alexandre Hubner e Heloisa Jahn.

PINHEIRO, Patrícia Peck. **Proteção de Dados Pessoais**: Comentários à lei nº 13.709/2018 (LGPD). São Paulo: Saraiva Educação, 2018. *E-book*.

RODOTÀ, Stefano. **A vida na sociedade de vigilância**. Rio de Janeiro: Renovar, 2008

SALGADO, Valéria Alpino Bigonha. **Ouvidorias do Poder Executivo Federal**. 2013. Disponível em: <https://www.cgu.gov.br/assuntos/ouvidoria/produtos-e-servicos/consulta-publica/arquivos/produto3_ouvidorias_executivo.pdf >. Acesso em 13 de setembro de 2020.

SANTOS, Fabíola Meira de Almeida; TALIBA, Rita. Lei Geral de Proteção de Dados no Brasil e os possíveis impactos. **Revista dos Tribunais** | vol. 998/2018 | p. 225 - 239 | Dez / 2018.

SCOPEL, Adriano Sayão. Breves considerações sobre tratamento de dados pelo Poder Público e meios de defesa dos dados pessoais por particulares. **Revista de Direito e as Novas Tecnologias** | vol. 7/2020 | Abr - Jun / 2020.

SILVA, Paulo Henrique Tavares da. e SOUSA, Rosilene Paiva Marinho de. Proteção de dados pessoais e os contornos da autodeterminação informativa. **Inf. & Soc.: Est**. João Pessoa, v.30, n.2, p. 1-19, abr./jun. 2020.

WARREN, Samuel D. BRANDEIS, Louis D. The right to privacy. p. 193-220. **Harvard Law Review**. Vol. 4, No. 5. (Dec. 15, 1890)

# ANÁLISE DA JURISPRUDÊNCIA DO TJPR



## Apresentação

A Revista da Ouvidoria, no propósito de fornecer ao usuário do serviço público informações relevantes acerca do sentido da jurisprudência e, por esse meio, propiciar elementos para a pauta de comportamentos na vida em sociedade, trata nesta seção da análise da jurisprudência do Tribunal de Justiça do Paraná, em torno da proteção de dados pessoais.

A Lei de Proteção de dados pessoais (Lei n.º 13709/2018) também conhecida pela siga LGPD, constituirá marco legal no direito brasileiro de grande impacto, tanto para as instituições privadas como para as públicas, na medida em que regula a proteção de dados pessoais de indivíduos em qualquer relação que envolva o tratamento de informações classificadas como dados pessoais. Com o intuito de fortalecer a proteção dos direitos fundamentais do titular de dados, a Lei n. 13.709/2018, pautou-se em inúmeros dispositivos previstos na Constituição Brasileira, podendo ser citados principalmente os artigos 3º, I e II; art. 4º, II; art. 5º, X e XII, art. 7º XXVII; e art. 219.

Trata-se de, mediante análise jurisprudencial do direito a proteção de dados pessoais, compreender os desafios para a aplicabilidade da norma, a partir de julgados do Tribunal de Justiça do Paraná. Não é o caso, obviamente, de aplicação de dispositivos específicos da LGPD, dado que ela entrou em vigor recentemente, mas de julgados que levam em conta casos envolvendo a proteção de dados pessoais à luz da legislação existente na época.

Para o efeito de compreensão da análise é interessante observar que o artigo 4º da LGDP delimita os tipos de dados protegidos, no contexto de fornecimento de bens ou serviços. Já o artigo 5º da LGDP especifica os termos utilizados na situação de dados pessoais, bem como os processos, técnicas ou procedimentos relativos ao tratamento de dados. A partir desses elementos, estabeleceu-se o alcance da tutela dos casos submetidos a apreciação do Tribunal de Justiça do Paraná, de modo a permitir verificar que, antes da entrada em vigor da LGPD, a jurisprudência da Corte buscava sistematizar a tutela de proteção de dados pessoais.

O avanço da tecnologia informática, e das consequentes plataformas de dados, exigiu a criação de mecanismos legais de regulamentação e proteção dos dados pessoais, de acordo com o contexto da cultura digital.

Assim, o interesse na análise da jurisprudência do Tribunal de Justiça do Paraná, a respeito da proteção de dados pessoais, se revela útil em dois aspectos: o primeiro na linha de proteção da pessoa sujeita as necessidades de uso da tecnologia informática e digital, e o segundo voltado para a compreensão das necessidades de adaptação as formas de proteção de dados por parte de organizações e empresas derivados das normas incluídas na LGDP.

## Metodologia

A busca da jurisprudência no Tribunal de Justiça de Paraná ocorreu por meio do sítio da internet: https://portal.tjpr.jus.br/jurisprudencia/. Para a busca foram utilizadas palavras-chave referidas a proteção de dados abrangidos por institutos agora incluídos na Lei Geral de Proteção de Dados Pessoais (LGPD). Foram utilizadas as seguintes palavras-chave: "Proteção de dados"; "Sigilo"; "Proteção à imagem"; "Violação de Sigilo de Dados" e "Armazenamento de Dados".

O período de pesquisa está compreendido entre agosto de 2019 e agosto de 2020.

A pesquisa realizada identificou **20** decisões proferidas pelo Tribunal de Justiça no período escolhido.

## Análise das decisões

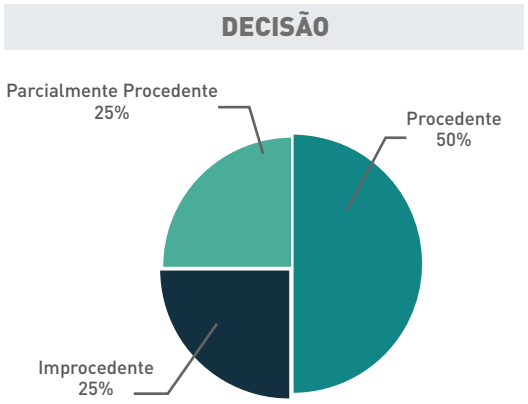
A análise tem como base os dados como perfil das partes, procedência ou improcedência da ação, e os motivos da judicialização do caso.

## Alcance normativo das decisões proferidas pelo Tribunal

Dentro da amostragem observou-se que 50% das decisões foram procedentes, no sentido de acolher o pedido da parte, 25% improcedentes, de não colhimento e 25% parcialmente procedentes, ou seja, de acolhimento parcial.

A partir da análise do gráfico, é possível visualizar o alto índice de ações julgadas procedentes, demostrando que o Tribunal de Justiça do Paraná, apesar da lacuna legislativa sobre os temas agora regidos pela LGPD, tem atuado para assegurar a proteção de dados pessoas no ambiente digital, articulado como categoria de direitos fundamentais.






As decisões de procedência do pedido diziam respeito aos seguintes temas:

- fornecimento de dados cadastrais;
- direito de imagem;
- quebra de sigilo fiscal;
- consulta aos sistemas renajud e infojud; e
- divulgação de informações pessoais.

Na Apelação Cível de nº 0007453-56.2018.8.16.0014, julgada pela 6ª Câmara Cível é possível verificar que o entendimento pela ilicitude da conduta praticada ofendia o arcabouço normativo de proteção da privacidade e intimidade na rede mundial de computadores, como a inviolabilidade do sigilo dos dados consoante o art. 5º, inciso XII, da CF, levando em conta a restrição de acesso às informações pessoais mantidas por instituições públicas e privadas, consoante o artigo 3º, inciso III do marco civil da internet (Lei 12.965/2014).

Por outro lado, a mera disponibilização pública, sem prévia anuência dos dados pessoais do autor na rede mundial de computadores, conforme agora regulado pela LGPD, ofende a privacidade e a intimidade da pessoa, privando-a da liberdade de definir a extensão do acesso a informações pessoas na internet, conforme se observa do sentido do julgado:

> *DIREITO CIVIL E PROCESSUAL CIVIL. APELAÇÃO CÍVEL EM NOMINADA "AÇÃO DE OBRIGAÇÃO DE FAZER CUMULADA COM PEDIDO DE INDENIZAÇÃO POR*

*DANOS MORAIS E TUTELA PROVISÓRIA DE URGÊNCIA ANTECIPADA". SENTENÇA DE PARCIAL PROCEDÊNCIA. RECURSO DO AUTOR: (1) DANO MORAL – CONFIGURADO – DIVULGAÇÃO DAS INFORMAÇÕES PESSOAIS DO AUTOR NA REDE MUNDIAL DE COMPUTADORES QUE OFENDE O DIREITO À PRIVACIDADE E À INTIMIDADE – DANO MORAL IN RE IPSA – DECORRÊNCIAS ESPECÍFICAS, TAIS COMO A EFETIVA UTILIZAÇÃO DOS DADOS POR TERCEIROS, QUE DEVEM SER LEVADAS EM CONTA APENAS NA QUANTIFICAÇÃO DA INDENIZAÇÃO, NÃO SENDO RELEVANTES PARA A CONFIGURAÇÃO DA LESÃO EXISTENCIAL – CASO CONCRETO QUE DENOTA A RAZOABILIDADE DA FIXAÇÃO DO MONTANTE EM R$ 5.000,00 (CINCO MIL REAIS). (2) ÔNUS DA SUCUMBÊNCIA – REDISTRIBUIÇÃO – RÉ QUE, ANTE A REFORMA DA SENTENÇA, DEVE ARCAR COM A TOTALIDADE DOS ÔNUS SUCUMBENCIAIS. RECURSOS CONHECIDO E PROVIDO.*

*(TJPR - 6ª C.Cível - 0007453-56.2018.8.16.0014 - Londrina - Rel.: Desembargador Renato Lopes de Paiva - J. 06.04.2020)*

*Link:***https://portal.tjpr.jus.br/jurisprudencia/j/4100000012515541/Ac%C3%B3rd%C3%A3o-0007453-56.2018.8.16.0014.**

Na linha de proteção de dados como direito fundamental da pessoa humana é interessante observar o que a 2.ª Câmara Criminal do Tribunal de Justiça do Paraná decidiu no julgamento da Apelação Criminal nº. 0005635-27.2017.8.16.0104:

*Apelação criminal. Usurpação de função pública qualificada – Artigo 328, parágrafo único, do Código Penal.1. Arguição de nulidade de interceptação telefônica – Não constatação – Providência adotada em estrita observância aos requisitos previstos na Lei n.º 9.296/1996 – Decisão de deferimento extensamente fundamentada, inclusive quanto à imprescindibilidade da medida – Interceptação telefônica, ademais, autorizada em procedimento investigatório que visava a apurar a prática de diversos delitos, inclusive apenados com reclusão – Irrelevância, portanto, de o crime imputado aos réus, em sua forma simples, em tese, ser punido com detenção – Mácula inexistente. 1.1. "É ônus da defesa, quando alega violação ao disposto no artigo 2º, inciso II, da Lei 9.296/1996, demonstrar que existiam, de fato, meios investigativos alternativos às autoridades para a elucidação dos fatos à época na qual a medida invasiva foi requerida, sob pena de a utilização da interceptação telefônica se tornar absolutamente inviável" (STJ, 5.ª Turma, RHC 62067-SP, Mussi).1.2. Não há negar a matriz que tem no sobreprincípio da dignidade da pessoa humana (CF, art. 1.º, inc. III) e sua estreita correlação com o direito subjetivo fundamental à privacidade (CF, art. 5.º, inc. X), o que exalça sobremaneira a garantia tanto por tanto constitucional do sigilo das comunicações (CF, art. 5.º, inc. XII). E o direito à privacidade, terminologia que nos vem do Direito Anglo-Americano (right of privacy), é amiúde considerado como sinônimo de direito à intimidade; afinal, no recôndito da privacidade se esconde a intimidade, não sendo despautério afirmar, também forte em prestigiada doutrina, que no âmbito da privacidade, a intimidade é o mais exclusivo de seus direitos.1.2.1. Conquanto o sigilo das comunicações seja direito fundamental (rectius: garantia fundamental), essa cláusula pétrea (CF, art. 60, § 2.º, inc. IV) (i) não possui caráter absoluto; vem daí que também por essa razão, quando em (ii) colisão com outros direitos fundamentais, reclama efetuação de juízo de ponderação, com preponderância, na situação então em avaliação, do bem jurídico com maior valoração.1.3. A Suprema Corte de Justiça do Brasil "consagrou o entendimento de que o princípio constitucional da inviolabilidade das comunicações (art. 5º, XII, da CF) não é absoluto, podendo o interesse público, em situações excepcionais, sobrepor-se aos direitos individuais para evitar que os direitos e garantias fundamentais sejam utilizados para acobertar condutas criminosas" (STF, RHC 115983-RJ, Lewandowski).1.4. É que os princípios jurídicos são espécies normativas com alto grau de generalidade. Diferentemente das regras jurídicas, os princípios são mandamentos de otimização, para empregar expressão muito ao gosto de Robert Alexy. Como refere esse ilustre professor de Filosofia do Direito da Universidade de Kiel (Alemanha), princípios são normas que ordenam que algo seja realizado na maior medida possível, dentro das possibilidades jurídicas e reais existentes.1.4.1. É por isso que os princípios reclamam ponderação: "[...] los principios son susceptibles de ponderación y, además, la necesitan. La ponderación es la forma de aplicación del derecho que caracteriza a los principios", explica Alexy. Em sua feliz síntese, "[...] los principios pueden y deben ser ponderados".1.4.2. Paralelamente ao reconhecimento científico uniforme de que os princípios podem e devem sofrer ponderação, não se pode deslembrar que os direitos fundamentais podem sofrer restrições. Alexy adverte que é quase trivial a ideia de que direitos tenham*

*restrições: "El concepto de restricción de un derecho nos parece familiar y no problemático. Que los derechos están sujetos a restricciones y pueden ser delimitados o limitados parece ser un conocimiento evidente y hasta trivial que en la Ley Fundamental se manifiesta con toda claridad cuando habla expresamente de restricciones [...], limitaciones [...], delimitaciones [...]".1.5. É exatamente o que se passa com a Constituição do Brasil, especificamente no que atina às comunicações telefônicas de que aqui se trata: o constituinte de 1988, ao tempo em que estabeleceu o princípio da inviolabilidade, restringiu, do mesmo passo, sua realização (do princípio), estipulando que ele não tem aplicação no caso ali indicado.1.5.1 Seja: o inciso XII do artigo 5.º da Lei Fundamental do Brasil prescreve que "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" (destaquei).2. Violação ao princípio do promotor natural – Procedimento investigativo instaurado pelo Grupo de Atuação Especial de Combate ao Crime Organizado (Gaeco) de Guarapuava, após a colheita de indícios pela Promotoria de Justiça de Cantagalo, dando conta da suspeita da existência de uma organização criminosa junto à Receita Estadual de Laranjeiras do Sul – Gaeco que tem como atribuição coordenar e impulsionar as atividades desenvolvidas para repressão a organizações criminosas, incluindo a instauração de procedimento investigatório criminal – Atribuições do Grupo Especial que são concorrentes às dos promotores de justiça que oficiam nas comarcas – Resolução n.º 1.807/2017, da Procuradoria-Geral de Justiça – Irrelevância do fato de, ao final do procedimento investigatório, não ter sido constatada a efetiva existência de organização criminosa – Vício não constatado – Precedentes do Superior Tribunal de Justiça.2.1. A atuação do Gaeco de Guarapuava, em atenção às suas atribuições previamente estabelecidas, estava amparada na probabilidade da existência de organização criminosa no âmbito da Receita Estadual de Laranjeiras do Sul, sendo irrelevante o fato de, ao final do procedimento investigatório, não ter sido constatada a efetiva existência desta.2.2. "É consolidado nos Tribunais Superiores o entendimento de que a atuação de promotores auxiliares ou de grupos especializados (GAECO) não ofende o princípio do promotor natural, uma vez que, nessa hipótese, amplia-se a capacidade de investigação,*



*de modo a otimizar os procedimentos necessários à formação da opinio delicti do Parquet" (STJ, 5.ª Turma, RHC 77422-RJ, Fonseca).3. Arguição de violação ao princípio da correlação – Não verificação – Decreto condenatório que se amolda perfeitamente aos fatos imputados na denúncia – Nulidade inexistente. 3.1. O princípio da correlação dispõe que deve haver identidade entre o objeto da imputação e o da sentença, i.e., o acusado deve ser julgado pelos fatos constantes da denúncia ou queixa-crime, sob pena de malferimento aos princípios da ampla defesa e do devido processo legal.4. Pretensão de absolvição quanto à prática do delito tipificado no artigo 328, parágrafo único, do Código Penal – Impossibilidade – Autoria e materialidade amplamente demonstradas – Relatos dos sujeitos passivos secundários de que o réu usurpou função pública, identificando-se e exercendo atos privativos a auditores fiscais da Receita Estadual, com o consentimento da acusada, visando a auferir vantagens indevidas dos contribuintes a título de tributos estaduais – Prova documental e interceptações telefônicas que também demonstram a prática delitiva – Elementos probatórios que evidenciam, indene de dúvida, a autoria e a materialidade delitiva – Perfeita subsunção dos fatos à norma penal – Precedentes desta Corte – Sentença condenatória mantida4.1. A prova oral produzida em Juízo, aliada àquelas atinentes à fase inquisitorial, demonstra que estão presentes todas as elementares do delito em análise, impondo-se a manutenção da condenação dos réus pelo crime tipificado no artigo 3.º, inciso II, da Lei n.º 8.137/1990.5. Desclassificação do crime de usurpação de função pública para a contravenção penal de simulação da qualidade de funcionário público – Impossibilidade – Circunstâncias do caso concreto que demonstram a prática do delito de usurpação de função pública, não da contravenção penal de simulação da qualidade de funcionário público. 5.1. O crime de usurpação de função pública exige para a sua caracterização que o agente assuma função pública e execute atos inerentes ao ofício, sem que tenha sido legalmente investido, para tanto, em cargo público.5.2. A contravenção penal de simulação da qualidade de funcionário público configura-se quando o agente se intitula funcionário público, sem que tenha praticado atos inerentes ao cargo.6. Incidência da circunstância agravante prevista no artigo 61, inciso II, alínea "g", do Código Penal em relação à corré M B P – Possibilidade – Delito em análise que não exige a qualidade de servidor público – Violação ao dever funcional que não*

*constitui elementar da norma penal incriminadora primária em análise – Viabilidade de incremento da pena – Manutenção da agravante que se impõe.7. Pena restritiva de direito, de prestação pecuniária – Necessidade de redução do valor arbitrado a tal título – Fixação em patamar superior ao mínimo legal sem fundamentação idônea e concreta – Situação econômica dos réus, que embora permita a fixação acima do mínimo, demandaria hígida fundamentação a esse respeito, inexistente no caso – Precedentes desta Corte.8. Pena de multa – Ausência de fixação do valor unitário do dia-multa na sentença – Vício que se sana, de ofício. 9. Recurso parcialmente provido.*

*(TJPR - 2ª C.Criminal - 0005635-27.2017.8.16.0104 - Laranjeiras do Sul - Rel.: Desembargador Rabello Filho - J. 22.08.2019)*

*Link:*https://portal.tjpr.jus.br/jurisprudencia/j/4100000007762951/Ac%C3%B3rd%C3%A3o-0005635-27.2017.8.16.0104#

Já as decisões de improcedência do pedido estavam relacionadas a causas que tratam dos seguintes temas:

- quebra de sigilo de dados telefônicos;
- armazenamento de dados;
- acesso a dados pessoais;
- fornecimento de dados.

Na Apelação Cível n.º 0028618-43.2014.8.16.0001 buscou-se aferir a legitimidade da crítica jornalística na relação com o interesse público, observada a razoabilidade dos meios e formas de divulgação da notícia devendo ser considerado abusivo o exercício daquelas liberdades sempre que identificada, em determinado caso concreto, a agressão aos direitos da pessoa, em particular relacionado aos dados de imagem; veja-se a ementa do julgado:

*APELAÇÃO CÍVEL. AÇÃO DE OBRIGAÇÃO DE FAZER CUMULADA COM DANOS MORAIS. LIBERDADE DE IMPRENSA VERSUS DIREITOS DA PERSONALIDADE: IMAGEM, HONRA, INTIMIDADE E VIDA PRIVADA. NOTÍCIA DA PRISÃO DOS AUTORES EM VÁRIOS SITES NOTICIOSOS. PEDIDO DE INDENIZAÇÃO POR DANO MORAL E DE EXCLUSÃO DAS NOTÍCIAS. PRETENDIDA RESPONSABILIZAÇÃO DAS EMPRESAS NOTICIOSAS E DO SITE DE BUSCAS. I. LEGITIMIDADE PASSIVA DO SITE QUE DISPONIBILIZA FERRAMENTA DE PESQUISA E INDICA LINKS ONDE SÃO ENCONTRADOS OS TERMOS FORNECIDOS PELO USUÁRIO. CARACTERIZAÇÃO, DIANTE DO PEDIDO DE SUPRESSÃO DOS LINKS, PARA EVITAR O ACESSO DOS USUÁRIOS ÀS MATÉRIAS. II. PRETENSA RESPONSABILIDADE DOS SITES NOTICIOSOS. PREMISSAS DA RESPONSABILIZAÇÃO CIVIL NÃO CARACTERIZADAS. AUSÊNCIA DE ABUSO NA VEICULAÇÃO DA NOTICIA. MERA REPRODUÇÃO DE INFORMATIVO DIVULGADO PELA AUTORIDADE POLICIAL RESPONSÁVEL PELA INVESTIGAÇÃO E PELA PRISÃO DOS AUTORES. AUSÊNCIA DE LEVIANDADE OU DIVULGAÇÃO DISTORCIDAS DAS INFORMAÇÕES OBTIDAS DA AUTORIDADE POLICIAL. DIVULGAÇÃO DE IMAGENS DO INTERIOR DA RESIDÊNCIA DOS AUTORES, POR OCASIÃO DA DILIGÊNCIA POLICIAL. AUSÊNCIA DE CONTEÚDO CONSTRANGEDOR OU VIOLADOR DOS DIREITOS DE PERSONALIDADE DOS AUTORES, NO CASO CONCRETO. INSURGÊNCIA, ADEMAIS, GENÉRICA. ATUAÇÃO REGULAR DAS REQUERIDAS, NO EXERCÍCIO DA SUA ATIVIDADE INFORMATIVA, AO DIVULGAR A PRISÃO DOS AUTORES. AUSÊNCIA DE ILICITUDE DA CONDUTA. DEVER DE INDENIZAR INEXISTENTE. III. SITE DE BUSCA. AUSÊNCIA DE INGERÊNCIA NO CONTEÚDO DAS INFORMAÇÕES VEICULADAS POR TERCEIROS. MERO MECANISMO DE PESQUISA. HIPÓTESE, ADEMAIS, DE NÃO IMPUGNAÇÃO DO CONTEÚDO PELO INTERESSADO. IV. DIREITO AO ESQUECIMENTO E DIREITO COLETIVO À INFORMAÇÃO. NECESSÁRIA ANÁLISE DAS CIRCUNSTÂNCIAS DO CASO CONCRETO E ULTERIOR PONDERAÇÃO SOB O PRISMA DA RAZOABILIDADE. PRETENSÃO DE EXCLUSÃO DAS NOTÍCIAS DE SUA PRISÃO. POSSIBILIDADE. ABSOLVIÇÃO POSTERIOR DOS AUTORES APELANTES DA IMPUTAÇÃO DA PRÁTICA DELITIVA. DECURSO DE CONSIDERÁVEL LAPSO TEMPORAL E AUSÊNCIA DE INTERESSE PÚBLICO NO CASO A JUSTIFICAR A MANUTENÇÃO DA VINCULAÇÃO DA NOTÍCIA À BUSCA PELOS NOMES DOS AUTORES E SUA ALCUNHA PROFISSIONAL. DESVINCULAÇÃO, ADEMAIS, QUE CONCILIA O DIREITO INDIVIDUAL E O DIREITO COLETIVO À INFORMAÇÃO. RECURSO PARCIALMENTE PROVIDO. "(...) No julgamento da ADPF 130, o STF proibiu enfaticamente a censura de publicações jornalísticas, bem como tornou excepcional qualquer tipo de intervenção estatal na divulgação de notícias e de opiniões. 3. A liberdade de expressão desfruta de uma posição preferencial no Estado democrático brasileiro, por ser uma pré-condição para o exercício esclarecido dos demais direitos e liberdades. 4. Eventual*

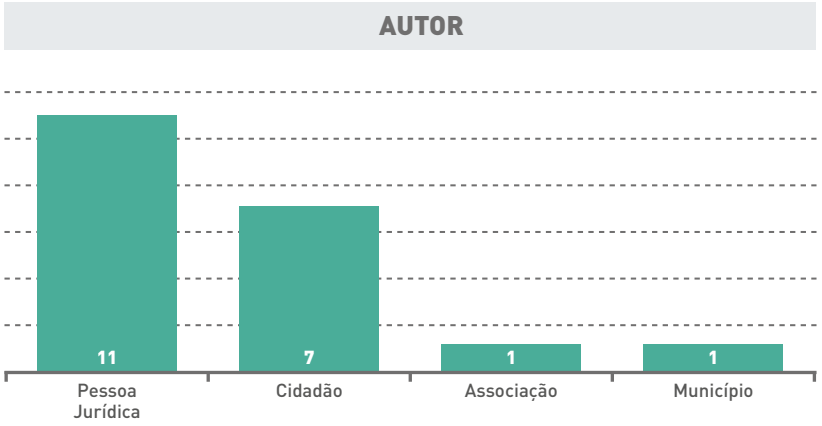
*uso abusivo da liberdade de expressão deve ser reparado, preferencialmente, por meio de retificação, direito de resposta ou indenização. (...) (STF-1ª Turma, Rcl 22.328, Relator Min. Roberto Barroso, j. 06/03/2018) "(...)A liberdade de imprensa é assegurada constitucionalmente, abrangendo os direitos de informar, informar-se e ser informado, devendo serem observados na notícia e respectiva crítica os pilares de cuidado, pertinência e veracidade. ADPF 130.2. Eventual abuso no direito de expressão pelos profissionais de imprensa deverão ser apurados à luz da legislação cível, de acordo com o caso concreto. Precedentes do STJ. (STJ-4ª Turma, AgInt no REsp 1678786/SP, Rel. Ministro Luis Felipe Salomão, j. 30/08/2018) "(...)Se, por um lado, não se permite a leviandade por parte da imprensa e a publicação de informações absolutamente inverídicas que possam atingir a honra da pessoa, não é menos certo, por outro lado, que da atividade jornalística não são exigidas verdades absolutas, provadas previamente em sede de investigações no âmbito administrativo, policial ou judicial" (STJ-4ª Turma, REsp 1473393/SP, Rel. Ministro Luis Felipe Salomão, j. 04/10/2016) "(...) A jurisprudência do Superior Tribunal de Justiça entende que a responsabilidade dos provedores de conteúdo de internet em geral depende da existência ou não do controle editorial do material disponibilizado na rede. No presente caso, a Corte de origem entendeu que não havia ingerência sobre o conteúdo, sendo a responsabilização indevida. Incidência da Súmula 83/STJ. (...) (STJ-4ª Turma, AgInt no REsp 1647548/MT, Rel. Ministro Lázaro Guimarães, j. 15/05/2018) "(...)A jurisprudência do Superior Tribunal de Justiça define que (a) para fatos anteriores à publicação do Marco Civil da Internet, basta a ciência inequívoca do conteúdo ofensivo pelo provedor, sem sua retirada em prazo razoável, para que este se torne responsável e, (b) após a entrada em vigor da Lei nº 12.965/2014, o termo inicial da responsabilidade solidária do provedor é o momento da notificação judicial que ordena a retirada do conteúdo da internet. (...) (STJ-3ª Turma, AgInt no REsp 1591179/CE, Rel. Ministro Ricardo Villas Bôas Cueva, j. 12/08/2019) "(...)15. Ao crime, por si só, subjaz um natural interesse público, caso contrário nem seria crime, e eventuais violações de direito resolver-se-iam nos domínios da responsabilidade civil. E esse interesse público, que é, em alguma medida, satisfeito pela publicidade do processo penal, finca raízes essencialmente na fiscalização social da resposta estatal que será dada ao fato. Se é assim, o interesse público que orbita o fenômeno criminal tende a desaparecer na medida em que também se esgota a resposta penal conferida ao fato criminoso, a qual, certamente, encontra seu último suspiro, com a extinção da pena ou com a absolvição, ambas consumadas irreversivelmente. E é nesse interregno temporal que se perfaz também a vida útil da informação criminal, ou seja, enquanto durar a causa que a legitimava. Após essa vida útil da informação seu uso só pode ambicionar, ou um interesse histórico, ou uma pretensão subalterna, estigmatizante, tendente a perpetuar no tempo as misérias humanas. (...) 17. Ressalvam-se do direito ao esquecimento os fatos genuinamente históricos - historicidade essa que deve ser analisada em concreto -, cujo interesse público e social deve sobreviver à passagem do tempo, desde que a narrativa desvinculada dos envolvidos se fizer impraticável. (...)" (STJ-4ª Turma, REsp 1334097/RJ, Rel. Ministro Luis Felipe Salomão, j. 28/05/2013) "(...) Há, todavia, circunstâncias excepcionalíssimas em que é necessária a intervenção pontual do Poder Judiciário para fazer cessar o vínculo criado, nos bancos de dados dos provedores de busca, entre dados pessoais e resultados da busca, que não guardam relevância para interesse público à informação, seja pelo conteúdo eminentemente privado, seja pelo decurso do tempo. 5. Nessas situações excepcionais, o direito à intimidade e ao esquecimento, bem como a proteção aos dados pessoais deverá preponderar, a fim de permitir que as pessoas envolvidas sigam suas vidas com razoável anonimato, não sendo o fato desabonador corriqueiramente rememorado e perenizado por sistemas automatizados de busca. 6. O rompimento do referido vínculo sem a exclusão da notícia compatibiliza também os interesses individual do titular dos dados pessoais e coletivo de acesso à informação, na medida em que viabiliza a localização das notícias àqueles que direcionem sua pesquisa fornecendo argumentos de pesquisa relacionados ao fato noticiado, mas não àqueles que buscam exclusivamente pelos dados pessoais do indivíduo protegido. (STJ-3ª Turma, REsp 1660168/RJ, Rel. Ministra Nancy Andrighi, Rel. p/ Acórdão Ministro Marco Aurélio Bellizze, j. 08/05/2018)*

*(TJPR - 6ª C.Cível - 0028618-43.2014.8.16.0001 - Curitiba - Rel.: Desembargadora Lilian Romero - J. 21.07.2020).*

*Link:* **https://portal.tjpr.jus.br/jurisprudencia/j/4100000010111771/Ac%C3%B3rd%C3%A3o-0028618-43.2014.8.16.0001#**

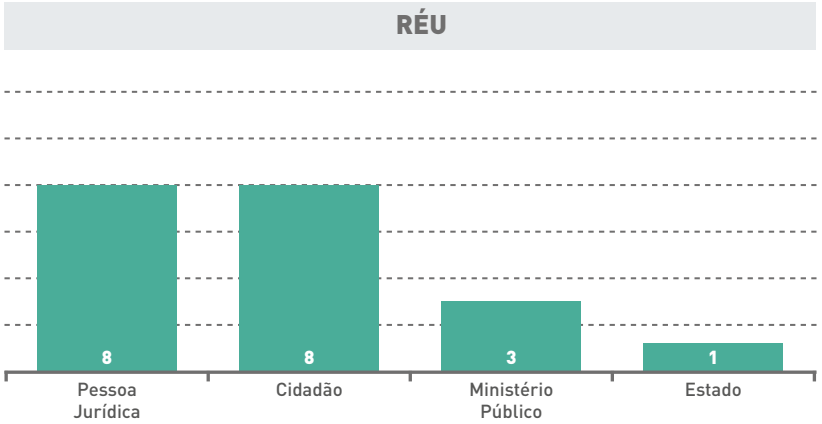
## Perfil do autor e do réu

A análise dos casos demostra diversidade de segmentos interessados na tutela do direito à proteção dos dados.




O gráfico mostra que, dos 20 (vinte) julgados analisados, 11 (onze) autores são pessoa jurídica de direito privado, diretamente relacionados ao próprio desenvolvimento do modelo de negócios da economia digital, que acaba por evidenciar que mudanças políticas, sociais e econômicas demandam o reconhecimento de novos direitos.

Em relação aos réus nas demandas também ocorre diversidade.






O dado que chama a atenção são as ações que tem como réu o Ministério Público que pode encontrar justificativa no protagonismo investigativo da instituição no combate ao crime organizado e na proteção do Estado.

Nesse sentido, no exame da Apelação Criminal dos autos de nº0029015-66.2014.8.16.0013, a 4ª Câmara Criminal entendeu que a mera verificação do telefone celular não configura quebra de sigilo de dados telefônicos ou violação a intimidade, conforme consta da ementa do julgado:

> *APELAÇÃO CRIME. TRÁFICO DE ENTORPECENTES (ART. 33, CAPUT, DA LEI Nº 11.343/2006) (1º E 2º FATOS). POSSE ILEGAL DE ARMA DE FOGO E MUNIÇÕES (ART. 16 DA LEI 10.826/2003) (3º FATO). INSURGÊNCIA DA DEFESA. PRETENSÃO DE RECORRER EM LIBERDADE. NÃO CONHECIMENTO. SENTENÇA QUE AUTORIZOU O RÉU A RECORRER EM LIBERDADE. AUSÊNCIA DE INTERESSE RECURSAL. PRELIMINAR DE NULIDADE PROCESSUAL. ARGUIÇÃO DE PROVAS OBTIDAS ILICITAMENTE NÃO VERIFICADA. MERA VERIFICAÇÃO DO APARELHO CELULAR DA TESTEMUNHA, QUE NÃO CONFIGURA QUEBRA DE SIGILO DE DADOS TELEFÔNICOS OU VIOLAÇÃO A INTIMIDADE. QUESTIONAMENTO DOS POLICIAIS ACERCA DA ORIGEM DA DROGA EM SITUAÇÃO DE FLAGRÂNCIA. PRESCINDIBILIDADE DE ADVERTIR O INVESTIGADO ACERCA DE SEU DIREITO DE PERMANECER CALADO. PRELIMINARES REJEITADAS. PLEITO DE ABSOLVIÇÃO DO DELITO DE TRÁFICO DE ENTORPECENTES. IMPOSSIBILIDADE. AUTORIA E MATERIALIDADE DEVIDAMENTE CONFIGURADAS. CONDUTAS DE VENDER, TER EM DEPÓSITO E POSSUIR. PLEITO SUBSIDIÁRIO DE DESCLASSIFICAÇÃO PARA USO PRÓPRIO (ART. 28, DA LEI Nº 11.343/2006). IMPOSSIBILIDADE. VALIDADE DA PALAVRA DOS POLICIAIS NO DELITO DE TRÁFICO QUE POSSUI ELEVADO VALOR PROBATÓRIO. ELEMENTOS CONSTANTES NOS AUTOS QUE NÃO DEIXAM DÚVIDAS DE QUE A SUBSTÂNCIA APREENDIDA SE DESTINAVA AO TRÁFICO. CONDIÇÃO DE USUÁRIO QUE NÃO AFASTA A TRAFICÂNCIA. CONDENAÇÃO MANTIDA. DELITO DE POSSE IRREGULAR DE ARMA DE FOGO (ART. 16 DA LEI 10.826/2003). PEDIDO DE ABSOLVIÇÃO POR ATIPICIDADE DA CONDUTA. INADMISSIBILIDADE. CRIME DE PERIGO ABSTRATO, SENDO DESNECESSÁRIA A CONSTATAÇÃO DE PERIGO OU LESÃO À SEGURANÇA PÚBLICA. CONDUTA DE MANTER EM*

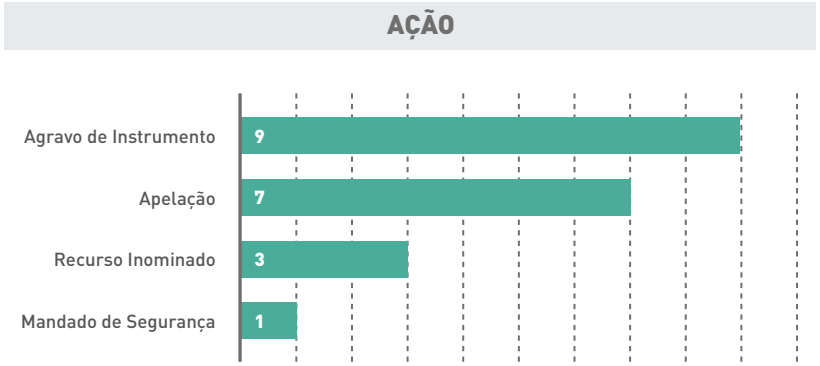
*DEPÓSITO O INSTRUMENTO SUFICIENTE PARA A INCIDÊNCIA DO TIPO. LAUDO PERICIAL QUE ATESTOU A PRESTABILIDADE E A EFICIÊNCIA DA ARMA. IMPOSSIBILIDADE DE APLICAÇÃO DO PRINCÍPIO DA INSIGNIFICÂNCIA AO PLEITO DE POSSE DE MUNIÇÃO DE USO RESTRITO. CONDENAÇÃO MANTIDA. DOSIMETRIA. PLEITO DE APLICAÇÃO DO PRIVILÉGIO CONTIDO NO §4ª DO ART. 33, DA LEI Nº 11.343/2006, EM SEU GRAU MÁXIMO. IMPOSSIBILIDADE. AUMENTO DEVIDAMENTE JUSTIFICADO. PRETENSÃO DE CUMPRIMENTO INICIAL DA PENA EM REGIME MAIS BRANDO. NÃO CABIMENTO. PENA FIXADA EM PATAMAR QUE AUTORIZA O CUMPRIMENTO DE PENA EM REGIME MAIS GRAVOSO. RECURSO PARCIALMENTE CONHECIDO E, NESSA EXTENSÃO, NÃO PROVIDO.*

*(TJPR - 4ª C.Criminal - 0029015-66.2014.8.16.0013 - Curitiba - Rel.: Desembargador Fernando Wolff Bodziak - J. 20.04.2020)*

*Link:*https://portal.tjpr.jus.br/jurisprudencia/j/4100000011256821/Ac%C3%B3rd%C3%A3o-0029015-66.2014.8.16.0013#

## Meios processuais utilizados pelos demandantes

A busca de proteção de dados no Tribunal de Justiça do Paraná utilizou dos recursos disponíveis, além da ação de mandado de segurança.






Como se observa, o recurso de agravo de instrumento é o mais utilizado, representado por 9 julgados.

Evidencia-se, desse modo, que a proteção de dados pessoais, com frequência, vem associada a disponibilização ou não de informações necessárias requeridas em sua maioria em sede de tutelas de urgência, o que explica dentro dos dados examinados, o alto índice de utilização dos agravos de instrumento. A busca de tutela de urgência é compatível com a dinâmica de rapidez e abrangência na operação da tecnologia digital.

A questão da urgência emerge na decisão proferida pela 5.ª Câmara Cível no Agravo de Instrumento nº 0025653-22.2019.8.16.0000:

*1) DIREITO PROCESSUAL CIVIL. TUTELA PROVISÓRIA DE URGÊNCIA. REQUISIÇÃO DIRETA, POR AUTORIDADE POLICIAL, SEM AUTORIZAÇÃO JUDICIAL, DE DADOS CADASTRAIS DE "IP" ("INTERNET PROTOCOL"). LEI DO MARCO CIVIL. FUMUS BONI JURIS E CARACTERIZADOS.PERICULUN IN MORA*

*a) A lei do marco civil da internet (Lei nº 12.965/14) resguarda o sigilo dos registros de conexão e de acesso à aplicações de internet, bem como de dados pessoais e do conteúdo de comunicações privadas, visando atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.*

*b) Assim, a disponibilização de tais dados pelo provedor, de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, como regra geral, somente se dará mediante ordem judicial (art. 10, § 1º).*

*c) A exceção de que trata o § 3º do art. 10, que autoriza a requisição dos dados cadastrais de forma direta "na forma da lei, pelas autoridades administrativas que detenham competência legal para a sua requisição", diz o que diz, e, segundo o próprio Relator do projeto de Lei, Deputado Alessandro Molon, a exceção foi concebida e incluída para que a regra geral pudesse conviver com leis anteriores que já contivessem previsão específica sobre a matéria (Lei nº 9.613/98- lavagem de dinheiro e 2.850/13, organizações criminosas).Lei nº*

*d) Assim, a princípio, numa interpretação lógico-sistemática, somente no âmbito das investigações regidas por estas leis específicas seria possível a requisição direta dos tais "dados cadastrais" ainda, que, nessas hipóteses, o provedor de conexão tenha que acessar outras informações do usuário para somente então, encaminhar à Autoridade Policial as informações que, na forma do inciso III do § 2º do art. 11 do Decreto nº 8.117/16, incluem: "III - a qualificação pessoal, entendida como nome, prenome, estado civil e profissão do usuário".*

*e) Ainda, a fim de preservar o trabalho policial de futuros questionamentos acerca da legitimidade da identificação de investigados feitas por requisições diretas, afigura-se prudente a concessão da tutela provisória de urgência, atrelando os pedidos de dados cadastrais à ordem judicial, exceto nos casos das leis específicas acima mencionadas.*

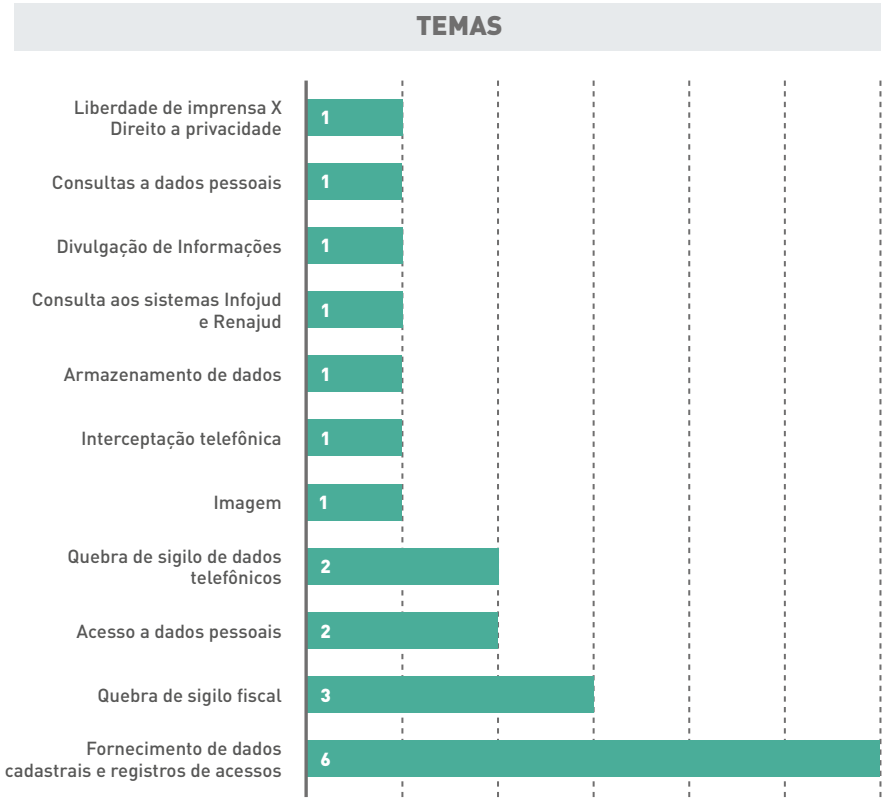
*2) AGRAVO DE INSTRUMENTO A QUE SE DÁ PROVIMENTO.*

*(TJPR - 5ª C.Cível - 0025653-22.2019.8.16.0000 - Curitiba - Rel.: Desembargador Carlos Mansur Arida - Rel.Desig. p/ o Acórdão: Desembargador Leonel Cunha - J. 10.12.2019).*

*Link:* https://portal.tjpr.jus.br/jurisprudencia/j/4100000009725241/Ac%C3%B3rd%C3%A3o-0025653-22.2019.8.16.0000#

## Temas da judicialização da proteção de dados

Em primeiro lugar a busca de tutela para a proteção de dados está relacionada ao fornecimento de dados cadastrais e registros de acessos, com 6 julgados. Em segundo lugar, outra questão frequente está relacionada a quebra de sigilo fiscal, em torno de demandas de execução e cumprimento de sentença na busca de bens para assegurar o pagamento de dívidas.




A busca pela proteção em torno do fornecimento de dados cadastrais e registro de acesso evidencia a preocupação da sociedade com a disponibilização de informações em meio digital, que constitui o ativo determinante das chamadas plataformas de dados, e seu papel no incremento de ganhos nos mercados na atualidade.

# PROTEÇÃO DE DADOS COM INDICATIVOS DE JURISPRUDÊNCIA



## Apresentação

A preocupação com a proteção de dados surge em virtude de reestruturação do poder, que, conforme Castells (1999), já não se concentra somente nas instituições tradicionais (Estado, Igrejas e Empresas), mas,

> *Difunde-se em redes globais de riqueza, informação e imagens, que circulam e se transmutam num sistema de geometria variável e geografia desmaterializada. No entanto, o poder não desaparece. O poder ainda governa a sociedade; ainda nos molda e domina (...) A nova forma de poder reside nos códigos da informação e nas imagens da representação em torno das quais as sociedades organizam as suas instituições e as pessoas constroem as suas vidas e decidem o seu comportamento. Esse poder encontra-se nas mentes das pessoas (CASTELLS, Manuel, A sociedade em rede, São Paulo, Paz e Terra, 1999, p.505-506).*

A comercialização de dados pessoais e sensíveis torna-se cada vez mais comum nas operações de plataforma e perigosa ao usuário no ambiente digital. Em razão do uso das informações coletadas tornou-se necessária uma legislação própria para tutelar esses direitos.

A Revista da Ouvidoria disponibiliza, nesta seção, indicativos dos posicionamentos jurisdicionai adotados pelas Cortes Superiores: STF, STJ e TRF4, acerca de decisões sobre a proteção de dados.

Antes da entrada em vigor da LGPD já havia um conjunto de normas sistematizador da proteção de dados pessoais no Brasil. Assim, o Poder Judiciário, no exercício da tutela de proteção e defesa do direito de proteção de dados, tem utilizado do Código Civil De 2002, do Código de Defesa do Consumidor, da Lei 12.737/2012 (Lei Carolina Dickmann) e da Lei n° 12.965/2014 (Marco Civil da Internet).

Os indicativos jurisprudenciais têm por objetivo informar o cidadão acerca do modo como o Poder Judiciário interpreta a legislação e busca proteger o direito de dados pessoais, com base das normas existentes antes da entrada em vigor LGPD.

Pela análise de casos julgados nas principais Cortes do país, procura-se fornecer ao leitor e usuário elementos de compreensão dos fundamentos jurídicos e fáticos de proteção de dados pessoais no ordenamento jurídico brasileiro.

# Metodologia

O critério de pesquisa jurisprudencial incluiu casos julgados pelo Supremo Tribunal Federal (STF), Superior Tribunal de Justiça (STJ) e Tribunal Regional Federal da 4º Região (TRF4).

Os julgados foram coletados por meio da internet, todos disponibilizados nos sítios dos tribunais pesquisados.

A busca foi realizada por meio de critérios delimitados por palavras-chave, no período mais recente de julgamento. As palavras escolhidas foram as seguintes: Banco de Dados; Compartilhamento de Dados; Dados Sigilosos; Marco Civil da Internet; Fornecimento de dados.

O período delimitado da pesquisa é anterior a entrada em vigor da LGPD e leva em conta os reflexos na decisão dos fundamentos jurídicos de proteção de dados pessoais no Brasil.

# STF

## Competência

De acordo com art. 102 da Constituição Federal Brasileira de 1988 (CF/88), compete ao STF o papel de guardião da Constituição. Assim, cabe-lhe julgar a ação direta de inconstitucionalidade de lei ou ato normativo federal ou estadual, a ação declaratória de constitucionalidade de lei ou ato normativo federal, a arguição de descumprimento de preceito fundamental decorrente da própria Constituição e a extradição solicitada por Estado estrangeiro**.**

Na esfera penal, destaca-se a competência para julgar, nas infrações penais comuns, o Presidente da República, o Vice-Presidente, os membros do Congresso Nacional, seus próprios Ministros e o Procurador-Geral da República, entre outros (art. 102, inc. I, a e b, da CF/1988).

O STF tem competência para julgar, em recurso ordinário, o *habeas corpus*, o mandado de segurança, o *habeas data* e o mandado de injunção decididos em única instância pelos Tribunais Superiores, se denegatória a decisão, e, em recurso extraordinário, as causas decididas em única ou última instância, quando a decisão recorrida contrariar dispositivo da Constituição.

## Decisões

**Tema de Repercussão Geral nº 990** - Possibilidade de compartilhamento com o Ministério Público, para fins penais, dos dados bancários e fiscais do contribuinte, obtidos pela Receita Federal no legítimo exercício de seu dever de fiscalizar, sem autorização prévia do Poder Judiciário.

EMENTA CONSTITUCIONAL. PROCESSUAL PENAL. COMPARTILHAMENTO COM O MINISTÉRIO PÚBLICO, PARA FINS PENAIS, DOS DADOS BANCÁRIOS E FISCAIS DO CONTRIBUINTE, OBTIDOS PELO FISCO NO LEGÍTIMO EXERCÍCIO DE SEU DEVER DE FISCALIZAR, SEM A INTERMEDIAÇÃO DO PODER JUDICIÁRIO. TRANSFERÊNCIA DE INFORMAÇÕES EM FACE DA PROTEÇÃO CONSTITUCIONAL DA INTIMIDADE E DO SIGILO DE DADOS. ART. 5º, INCISOS X E XII, DA CONSTITUIÇÃO FEDERAL. QUESTÃO EMINENTEMENTE CONSTITUCIONAL. MATÉRIA PASSÍVEL DE REPETIÇÃO EM INÚMEROS PROCESSOS, A REPERCUTIR NA ESFERA DO INTERESSE PÚBLICO. TEMA COM REPERCUSSÃO GERAL.

(RE 1055941 RG, Relator(a): DIAS TOFFOLI, Tribunal Pleno, julgado em 12/04/2018, DJe-083 DIVULG 27-04-2018 PUBLIC 30-04-2018)

Link:**https://jurisprudencia.stf.jus.br/pages/search/repercussao-geral9702/false**

**RE 601314 / SP - SÃO PAULO**

RECURSO EXTRAORDINÁRIO. REPERCUSSÃO GERAL. DIREITO TRIBUTÁRIO. DIREITO AO SIGILO BANCÁRIO. DEVER DE PAGAR IMPOSTOS. REQUISIÇÃO DE INFORMAÇÃO DA RECEITA FEDERAL ÀS INSTITUIÇÕES FINANCEIRAS. ART. 6º DA LEI COMPLEMENTAR 105/01. MECANISMOS FISCALIZATÓRIOS. APURAÇÃO DE CRÉDITOS RELATIVOS A TRIBUTOS DISTINTOS DA CPMF. PRINCÍPIO DA IRRETROATIVIDADE DA NORMA TRIBUTÁRIA. LEI 10.174/01.

1. O litígio constitucional posto se traduz em um confronto entre o direito ao sigilo bancário e o dever de pagar tributos, ambos referidos a um mesmo cidadão e de caráter

constituinte no que se refere à comunidade política, à luz da finalidade precípua da tributação de realizar a igualdade em seu duplo compromisso, a autonomia individual e o autogoverno coletivo.

2. Do ponto de vista da autonomia individual, o sigilo bancário é uma das expressões do direito de personalidade que se traduz em ter suas atividades e informações bancárias livres de ingerências ou ofensas, qualificadas como arbitrárias ou ilegais, de quem quer que seja, inclusive do Estado ou da própria instituição financeira.

3. Entende-se que a igualdade é satisfeita no plano do autogoverno coletivo por meio do pagamento de tributos, na medida da capacidade contributiva do contribuinte, por sua vez vinculado a um Estado soberano comprometido com a satisfação das necessidades coletivas de seu Povo.

4. Verifica-se que o Poder Legislativo não desbordou dos parâmetros constitucionais, ao exercer sua relativa liberdade de conformação da ordem jurídica, na medida em que estabeleceu requisitos objetivos para a requisição de informação pela Administração Tributária às instituições financeiras, assim como manteve o sigilo dos dados a respeito das transações financeiras do contribuinte, observando-se um translado do dever de sigilo da esfera bancária para a fiscal.

5. A alteração na ordem jurídica promovida pela Lei 10.174/01 não atrai a aplicação do princípio da irretroatividade das leis tributárias, uma vez que aquela se encerra na atribuição de competência administrativa à Secretaria da Receita Federal, o que evidencia o caráter instrumental da norma em questão. Aplica-se, portanto, o artigo 144, §1º, do Código Tributário Nacional.

6. Fixação de tese em relação ao item "a" do Tema 225 da sistemática da repercussão geral: "O art. 6º da Lei Complementar 105/01 não ofende o direito ao sigilo bancário, pois realiza a igualdade em relação aos cidadãos, por meio do princípio da capacidade contributiva, bem como estabelece requisitos objetivos e o translado do dever de sigilo da esfera bancária para a fiscal".

7. Fixação de tese em relação ao item "b" do Tema 225 da sistemática da repercussão geral: "A Lei 10.174/01 não atrai a aplicação do princípio da irretroatividade das leis tributárias, tendo em vista o caráter instrumental da norma, nos termos do artigo 144, §1º, do CTN". 8. Recurso extraordinário a que se nega provimento.

(RE 601314, Relator(a): EDSON FACHIN, Tribunal Pleno, julgado em 24/02/2016, ACÓRDÃO ELETRÔNICO REPERCUSSÃO GERAL - MÉRITO DJe-198 DIVULG 15-09-2016 PUBLIC 16-09-2016)

Link: **https://jurisprudencia.stf.jus.br/pages/search/sjur356216/false**

**RE 1037396 RG / SP - SÃO PAULO**

EMENTA Direito Constitucional. Proteção aos direitos da personalidade. Liberdade de expressão e de manifestação. Violação dos arts. 5º, incisos IV, IX, XIV; e 220, caput, §§ 1º e 2º, da Constituição Federal. Prática de ato ilícito por terceiro. Dever de fiscalização e de exclusão de conteúdo pelo prestador de serviços. Reserva de jurisdição. Responsabilidade civil de provedor de internet, websites e gestores de aplicativos de redes sociais. Constitucionalidade ou não do art. 19 do Marco Civil da Internet (Lei nº 12.965/14) e possibilidade de se condicionar a retirada de perfil falso ou tornar indisponível o conteúdo apontado como infringente somente após ordem judicial específica. Repercussão geral reconhecida.

(RE 1037396 RG, Relator(a): DIAS TOFFOLI, Tribunal Pleno, julgado em 01/03/2018, PROCESSO ELETRÔNICO DJe-063 DIVULG 03-04-2018 PUBLIC 04-04-2018)

Tema 987 - Discussão sobre a constitucionalidade do art. 19 da Lei n. 12.965/2014 (Marco Civil da Internet) que determina a necessidade de prévia e específica ordem judicial de exclusão de conteúdo para a responsabilização civil de provedor de internet, websites e gestores de aplicativos de redes sociais por danos decorrentes de atos ilícitos praticados por terceiros.

Link: **https://jurisprudencia.stf.jus.br/pages/search/repercussao-geral9662/false**

**ARE 660861 RG / MG - MINAS GERAIS**

EMENTA: GOOGLE – REDES SOCIAIS – SITES DE RELACIONAMENTO – PUBLICAÇÃO DE MENSAGENS NA INTERNET – CONTEÚDO OFENSIVO – RESPONSABILIDADE CIVIL DO PROVEDOR – DANOS MORAIS – INDENIZAÇÃO – COLISÃO ENTRE LIBERDADE DE EXPRES-

SÃO E DE INFORMAÇÃO vs. DIREITO À PRIVACIDADE, À INTIMIDADE, À HONRA E À IMAGEM. REPERCUSSÃO GERAL RECONHECIDA PELO PLENÁRIO VIRTUAL DESTA CORTE. (ARE 660861 RG, Relator(a): LUIZ FUX, Tribunal Pleno, julgado em 22/03/2012, PROCESSO ELETRÔNICO DJe-219 DIVULG 06-11-2012 PUBLIC 07-11-2012) .

Tema 533 - Dever de empresa hospedeira de sítio na internet fiscalizar o conteúdo publicado e de retirá-lo do ar quando considerado ofensivo, sem intervenção do Judiciário.

Link: https://jurisprudencia.stf.jus.br/pages/search/repercussao-geral4181/false

**ARE 652777 RG / SP - SÃO PAULO**

EMENTA: CONSTITUCIONAL. ADMINISTRATIVO. DIVULGAÇÃO, EM SÍTIO ELETRÔNICO OFICIAL, DE INFORMAÇÕES ALUSIVAS A SERVIDORES PÚBLICOS. CONFLITO APARENTE DE NORMAS CONSTITUCIONAIS. DIREITO À INFORMAÇÃO DE ATOS ESTATAIS. PRINCÍPIO DA PUBLICIDADE ADMINISTRATIVA. PRIVACIDADE, INTIMIDADE E SEGURANÇA DE SERVIDORES PÚBLICOS. Possui repercussão geral a questão constitucional atinente à divulgação, em sítio eletrônico oficial, de informações alusivas a servidores públicos.

(ARE 652777 RG, Relator(a): AYRES BRITTO, Tribunal Pleno, julgado em 29/09/2011, ACÓRDÃO ELETRÔNICO DJe-071 DIVULG 11-04-2012 PUBLIC 12-04-2012)

Tema 483 - Responsabilidade civil do Estado por dano moral decorrente de publicação da remuneração de servidor público em site na internet.

Link: https://jurisprudencia.stf.jus.br/pages/search/repercussao-geral3501/false

**RE 589257 AgR / DF - DISTRITO FEDERAL**

HABEAS DATA – DADOS DE CÔNJUGE FALECIDO – LEGITIMIDADE DO SUPÉRSTITE. Conforme alcance do artigo 5º, inciso LXXII, alínea "a" da Constituição Federal, é assegurado ao cônjuge supérstite o conhecimento de informações relativas ao falecido, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público.

RECURSO EXTRAORDINÁRIO – MATÉRIA FÁTICA E LEGAL. O recurso extraordinário não é meio próprio ao revolvimento da prova, também não servindo à interpretação de normas estritamente legais.



(RE 589257 AgR, Relator(a): MARCO AURÉLIO, Primeira Turma, julgado em 05/08/2014, ACÓRDÃO ELETRÔNICO DJe-164 DIVULG 25-08-2014 PUBLIC 26-08-2014)

Link: https://jurisprudencia.stf.jus.br/pages/search/sjur274042/false

**RE 673707 / MG - MINAS GERAIS**

Ementa: DIREITO CONSTITUCIONAL. DIREITO TRIBUTÁRIO. HABEAS DATA. ARTIGO 5º, LXXII, CRFB/88. LEI Nº 9.507/97. ACESSO ÀS INFORMAÇÕES CONSTANTES DE SISTEMAS INFORMATIZADOS DE CONTROLE DE PAGAMENTOS DE TRIBUTOS. SISTEMA DE CONTA CORRENTE DA SECRETARIA DA RECEITA FEDERAL DO BRASIL-SINCOR. DIREITO SUBJETIVO DO CONTRIBUINTE. RECURSO A QUE SE DÁ PROVIMENTO.

1. O habeas data, posto instrumento de tutela de direitos fundamentais, encerra amplo espectro, rejeitando-se visão reducionista da garantia constitucional inaugurada pela carta pós-positivista de 1988.

2. A tese fixada na presente repercussão geral é a seguinte: "O Habeas Data é 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."

3. O Sistema de Conta Corrente da Secretaria da Receita Federal do Brasil, conhecido também como SINCOR, registra os dados de apoio à arrecadação federal ao armazenar os débitos e créditos tributários existentes acerca dos contribuintes.

4. O caráter público de todo registro ou banco de dados contendo informações que sejam ou que possam ser transmitidas a terceiros ou que não sejam de uso privativo do órgão ou entidade produtora ou depositária das informações é inequívoco (art. 1º, Lei nº 9.507/97).

5. 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. (...) Registro de dados deve ser entendido em seu sentido mais amplo, abrangendo tudo que diga respeito ao interessado, seja de modo direto ou indireto, causando-lhe dano ao seu direito de privacidade.(...) in José Joaquim Gomes Canotilho, Gilmar Ferreira Mendes, Ingo Wolfgang Sarlet e Lenio Luiz Streck. Comentários à Constituição. Editora Saraiva, 1ª Edição, 2013, p.487.

6. A legitimatio ad causam para interpretação de Habeas Data estende-se às pessoas físicas e jurídicas, nacionais e estrangeiras, porquanto garantia constitucional aos direitos individuais ou coletivas.

7. Aos contribuintes foi assegurado constitucionalmente 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, verbis: Art. 5º. ...LXXII. Conceder-se-á habeas data 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, considerado como um writ, uma garantia, um remédio constitucional à disposição dos cidadãos para que possam implementar direitos subjetivos que estão sendo obstaculizados.

8. 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 sub examine, verbis: Art. 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.

9. In casu, o recorrente requereu à Secretaria da Receita Federal do Brasil os extratos atinentes às anotações constantes do Sistema de Conta-Corrente de Pessoa Jurídica-SINCOR, o Sistema Conta-Corrente de Pessoa Jurídica-CONTACORPJ, como de quaisquer dos sistemas informatizados de apoio à arrecadação federal, no que tange aos pagamentos de tributos federais, informações que não estão acobertadas pelo sigilo legal ou constitucional, posto que requerida pelo próprio contribuinte, sobre dados próprios.

10. Ex positis, DOU PROVIMENTO ao recurso extraordinário.



(RE 673707, Relator(a): LUIZ FUX, Tribunal Pleno, julgado em 17/06/2015, ACÓRDÃO ELETRÔNICO REPERCUSSÃO GERAL - MÉRITO DJe-195 DIVULG 29-09-2015 PUBLIC 30-09-2015)

Tema 582 - Cabimento de habeas data para fins de acesso a informações incluídas em banco de dados denominado SINCOR - Sistema de Conta-Corrente de Pessoa Jurídica, da Receita Federal.

Link: **https://jurisprudencia.stf.jus.br/pages/search/sjur322444/false**

**MS 31631 / SP - SÃO PAULO**

PROGRAMA JUSTIÇA PLENA – BANCO DE DADOS – ACESSO. O acesso, limitado, ao banco de dados do Programa Justiça Plena não vulnera direito do cidadão envolvido, como parte, em processo judicial. CONSELHO NACIONAL DE JUSTIÇA – ATUAÇÃO – JUDICATURA – INDEPENDÊNCIA. A atuação administrativa do Conselho Nacional de Justiça não consubstancia intimidação do magistrado no desempenho do ofício judicante.

(MS 31631, Relator(a): MARCO AURÉLIO, Primeira Turma, julgado em 15/08/2017, PROCESSO ELETRÔNICO DJe-190 DIVULG 25-08-2017 PUBLIC 28-08-2017)

RE 601766 AgR / MG - MINAS GERAIS

Link: **https://jurisprudencia.stf.jus.br/pages/search/sjur372068/false**

**AP 1030 AgR / DF - DISTRITO FEDERAL**

Ementa: AGRAVO REGIMENTAL. AÇÃO PENAL. INSTRUÇÃO CRIMINAL. PRETENSÃO DE ACESSO A MATERIAL PERICIADO. ACOLHIMENTO. QUEBRA DE SIGILO DE DADOS TELEFÔNICOS DO NÚCLEO DE INTELIGÊNCIA DA POLÍCIA FEDERAL. PRETENSÃO NÃO AMPARADA PELO ORDENAMENTO JURÍDICO. INDEFERIMENTO. INSURGÊNCIA PROVIDA, EM PARTE.

1. Efetivando a garantia à ampla defesa prevista no art. 5º, LV, da Constituição Federal, o legislador ordinário previu no art. 159, § 6º, do Código de Processo Penal a possibilidade de disponibilização às partes, mediante requerimento, do material probatório periciado, o que autoriza o deferimento, nesse ponto, da pretensão dos agravantes.

2. O pleito de quebra de sigilo de dados telefônicos do Núcleo de Inteligência da Polícia Federal não tem por objeto qualquer investigação da prática de uma infração penal, como exige a Lei 9.296/1996, mas apenas a ciência de quem seria o autor de notícia criminal que culminou com diligência de busca e apreensão. Assim, aos agravantes falta legitimidade ao exercício da pretensão, nos termos do art. 3º do aludido diploma legal, a qual também encontra óbice no art. 3º da Lei 13.608/2018, que protege o sigilo dos dados de informante que se utiliza de serviço telefônico de recebimento de denúncias.

3. Agravo regimental provido, em parte.

(AP 1030 AgR, Relator(a): EDSON FACHIN, Segunda Turma, julgado em 25/09/2018, ACÓRDÃO ELETRÔNICO DJe-032 DIVULG 15-02-2019 PUBLIC 18-02-2019)

Link:**https://jurisprudencia.stf.jus.br/pages/search/sjur398457/false**

**Rcl 25537 / DF - DISTRITO FEDERAL**

Ementa: RECLAMAÇÃO. AÇÃO CAUTELAR. JULGAMENTO CONJUNTO. MATÉRIA PROCESSUAL PENAL. BUSCA E APREENSÃO REALIZADA NAS DEPENDÊNCIAS DO SENADO FEDERAL. MEDIDA AUTORIZADA PELO JUÍZO DE PRIMEIRO GRAU. AUSÊNCIA DE AUTOMÁTICA E NECESSÁRIA USURPAÇÃO DA COMPETÊNCIA DO SUPREMO TRIBUNAL FEDERAL. SUPERVISÃO DE APURAÇÃO TENDENTE A ELUCIDAR CONDUTAS POTENCIALMENTE ATRIBUÍDAS A CONGRESSISTAS NO EXERCÍCIO DA FUNÇÃO PARLAMENTAR. VULNERAÇÃO À COMPETÊNCIA DESTA CORTE. HIGIDEZ DAS PROVAS REPETÍVEIS OU QUE DISPENSAM PRÉVIA AUTORIZAÇÃO JUDICIAL. PEDIDO PARCIALMENTE PROCEDENTE.

1. A competência penal originária do Supremo Tribunal Federal, inclusive no que toca à etapa investigatória, encontra-se taxativamente elencada nas regras de direito estrito estabelecidas no art. 102 da CRFB, razão pela qual não permite alargamento pela via interpretativa.

2. Inexistente previsão constitucional em direção diversa, não há como se acolher a pretensão no sentido de que seria necessariamente do Supremo Tribunal Federal a competência para apreciar pedido de busca e apreensão a ser cumprida nas dependências de Casas Legislativas. Isso porque, conforme se extrai do art. 102, CRFB, não se elegeu o local da realização de diligências, ou seja, o critério espacial, como fator de determinação de competência desta Corte.

3. As imunidades parlamentares visam a salvaguardar a independência do exercício dos respectivos mandatos congressuais, de modo que não são passíveis de extensão em favor de outros agentes públicos ou funções alheias às estritas atividades parlamentares. Por essa razão, não há impedimento normativo de que integrantes de Polícia Legislativa sejam diretamente investigados em primeiro grau, na medida em que referidas funções públicas não se inserem no rol taxativo a legitimar a competência penal originária desta Suprema Corte.

4. Eventuais interferências entre os Poderes constituídos ou condicionamentos da atividade jurisdicional, como a exigência de participação de outros órgãos na realização de determinadas diligências, devem decorrer de previsão constitucional, descabendo adotar mecanismo de freio e contrapeso não disciplinado, expressa ou implicitamente, pela própria Constituição da República.

5. A jurisprudência desta Suprema Corte firmou-se no sentido de que a competência penal constitucionalmente estabelecida alcança também a fase investigatória. Assim, se inexistir indicativo de competência do Supremo Tribunal Federal para processar e julgar eventual ação penal, não há razão para que a Suprema Corte aprecie medida de cunho preparatório e acessório.

6. Em sede de reclamação, a alegação de usurpação da competência do STF em razão da investigação, em primeiro grau, de agentes detentores de foro nesta Suprema Corte, deve ser demonstrada sem exigir o reexame de matéria fático-probatória. Para a configuração dessas circunstâncias, são insuficientes a possibilidade abstrata de envolvimento de parlamentares, bem como simples menções a nomes de congressistas.

7. Caso concreto em que, segundo decisões judiciais anteriormente proferidas pelo Juízo reclamado, a confirmação das hipóteses investigatórias poderia levar a identificação de parlamentares que, em tese, teriam comandado os atos objeto de apuração, cenário,

a um só tempo, a denotar a usurpação da competência desta Suprema Corte e afastar a alegação de incidência da Teoria do Juízo Aparente.

8. A irregularidade atinente à competência para supervisão das investigações não infirma a validade de quaisquer elementos probatórios não sujeitos à cláusula de reserva de jurisdição e que, bem por isso, dispensam, para sua produção ou colheita, prévia autorização judicial.

9. As interceptações telefônicas, por sua vez, sujeitas a perecimento por excelência, bem como a quebra de sigilo telefônico deferida com base nesses diálogos captados, são declaradas ilícitas em relação aos detentores de prerrogativa de foro nesta Corte, providência que não se estende aos demais investigados.

10. O Tribunal Pleno, por maioria, acolheu o pedido cautelar formulado pela Procuradoria-Geral da República para o fim de não desconstituir a busca e apreensão realizada, resguardando-se o exame exauriente da validade de eventuais provas decorrentes da medida para momento oportuno, após avaliação do material arrecadado pelos órgãos de persecução.

11. Pedido julgado parcialmente procedente.

(Rcl 25537, Relator(a): EDSON FACHIN, Tribunal Pleno, julgado em 26/06/2019, PROCESSO ELETRÔNICO DJe-052 DIVULG 10-03-2020 PUBLIC 11-03-2020)

Link: **https://jurisprudencia.stf.jus.br/pages/search/sjur420410/false**

**Rcl 25872 AgR-AgR / SP - SÃO PAULO**

AGRAVO REGIMENTAL EM AGRAVO REGIMENTAL EM RECLAMAÇÃO. SÚMULA VINCULANTE Nº 14. DADOS SIGILOSOS DE TERCEIROS. RESTRIÇÃO LEGÍTIMA DE ACESSO. IMPOSSIBILIDADE DE SUA UTILIZAÇÃO COMO ELEMENTO DE PROVA CONTRA O ACUSADO. AUSÊNCIA DE VIOLAÇÃO DO CONTRADITÓRIO E DA AMPLA DEFESA.

1. Não viola o enunciado da Súmula Vinculante nº 14 decisão que garante ao reclamante acesso aos elementos de prova já documentados nos autos, excluindo excertos que não atinjam sua esfera jurídica e contenham dados sigilosos de terceiros.



2. O direito à intimidade e ao sigilo de dados de terceiros gozam de proteção constitucional qualificada por cláusula de reserva de jurisdição, relativizada somente nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal (art. 5º, XII, CF/88).

3. A decisão combatida, a um só tempo, protege direitos fundamentais de terceiros e viabiliza o pleno exercício do direito de defesa pelos investigados e acusados, atendendo aos vetores da necessidade, adequação e proporcionalidade em sentido estrito.

4. Aquilo que não disser respeito ao investigado ou acusado e, por conseguinte, tiver sido excluído de seu âmbito de conhecimento, não poderá ser objeto de cognição judicial para fins de formação de eventual juízo condenatório contra si, o que afasta a alegação de prejuízo à sua esfera jurídica material ou processual.

5. Agravo regimental conhecido e não provido.

(Rcl 25872 AgR-AgR, Relator(a): ROSA WEBER, Primeira Turma, julgado em 17/12/2019, PROCESSO ELETRÔNICO DJe-047 DIVULG 05-03-2020 PUBLIC 06-03-2020)

Link: **https://jurisprudencia.stf.jus.br/pages/search/sjur420055/false**

**RE 418416 / SC - SANTA CATARINA**

EMENTA:

I. Decisão judicial: fundamentação: alegação de omissão de análise de teses relevantes da Defesa: recurso extraordinário: descabimento. Além da falta do indispensável prequestionamento (Súmulas 282 e 356), não há violação dos art. 5º, LIV e LV, nem do art. 93, IX, da Constituição, que não exige o exame pormenorizado de cada uma das alegações ou provas apresentadas pelas partes, nem que sejam corretos os fundamentos da decisão; exige, apenas, que a decisão esteja motivada, e a sentença e o acórdão recorrido não descumpriram esse requisito (v.g., RE140.370, 1ª T., 20.4.93, Pertence, DJ 21.5.93; AI 242.237 – AgR, 1ª T., 27.6.00, Pertence, DJ 22.9.00).

II. Quebra de sigilo bancário: prejudicadas as alegações referentes ao decreto que a determinou, dado que a sentença e o acórdão não se referiram a qualquer prova resultante

da quebra do sigilo bancário, tanto mais que, dado o deferimento parcial de mandado de segurança, houve a devolução da documentação respectiva.

III. Decreto de busca e apreensão: validade. Decreto específico, que somente permitiu que as autoridades encarregadas da diligência selecionassem objetos, dentre aqueles especificados na decisão e na sede das duas empresas nela indicadas, e que fossem "interessantes à investigação" que, no caso, tinha pertinência com a prática do crime pelo qual foi efetivamente condenado o recorrente. 2. Ademais não se demonstrou que as instâncias de mérito tenham invocado prova não contida no objeto da medida judicial, nem tenham valorado qualquer dado resultante da extensão dos efeitos da decisão determinante da busca e apreensão, para que a Receita Federal e a "Fiscalização do INSS" também tivessem acesso aos documentos apreendidos, para fins de investigação e cooperação na persecução criminal, "observado o sigilo imposto ao feito".

IV - Proteção constitucional ao sigilo das comunicações de dados - art. 5º, XVII, da CF: ausência de violação, no caso. 1. Impertinência à hipótese da invocação da AP 307 (Pleno, 13.12.94, Galvão, DJU 13.10.95), em que a tese da inviolabilidade absoluta de dados de computador não pode ser tomada como consagrada pelo Colegiado, dada a interferência, naquele caso, de outra razão suficiente para a exclusão da prova questionada - o ter sido o microcomputador apreendido sem ordem judicial e a conseqüente ofensa da garantia da inviolabilidade do domicílio da empresa - este segundo fundamento bastante, sim, aceito por votação unânime, à luz do art. 5º, XI, da Lei Fundamental. 2. Na espécie, ao contrário, não se questiona que a apreensão dos computadores da empresa do recorrente se fez regularmente, na conformidade e em cumprimento de mandado judicial. 3. Não há violação do art. 5º. XII, da Constituição que, conforme se acentuou na sentença, não se aplica ao caso, pois não houve "quebra de sigilo das comunicações de dados (interceptação das comunicações), mas sim apreensão de base física na qual se encontravam os dados, mediante prévia e fundamentada decisão judicial". 4. A proteção a que se refere o art.5º, XII, da Constituição, é da comunicação 'de dados' e não dos 'dados em si mesmos', ainda quando armazenados em computador. (cf. voto no MS 21.729, Pleno, 5.10.95, red. Néri da Silveira -RTJ 179/225, 270).



V - Prescrição pela pena concretizada: declaração, de ofício, da prescrição da pretensão punitiva do fato quanto ao delito de frustração de direito assegurado por lei trabalhista (C. Penal, arts. 203; 107, IV; 109, VI; 110, § 2º e 114, II; e Súmula 497 do Supremo Tribunal).

(RE 418416, Relator(a): SEPÚLVEDA PERTENCE, Tribunal Pleno, julgado em 10/05/2006, DJ 19-12-2006 PP-00037 EMENT VOL-02261-06 PP-01233)

Link: **https://jurisprudencia.stf.jus.br/pages/search/sjur92577/false**.

**RMS 24617 / DF - DISTRITO FEDERAL**

EMENTA: CONSTITUCIONAL. MANDADO DE SEGURANÇA. HABEAS DATA. C.F., ART. 5º, LXIX E LXXII. Lei 9.507/97, art. 7º, I.

I. - O habeas data tem finalidade específica: assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público, ou para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo (C.F., art. 5º, LXXII, a e b).

II. - No caso, visa a segurança ao fornecimento ao impetrante da identidade dos autores de agressões e denúncias que lhe foram feitas. A segurança, em tal caso, é meio adequado. Precedente do STF: MS 24.405/DF, Ministro Carlos Velloso, Plenário, 03.12.2003, "DJ" de 23.4.2004.

III. - Recurso provido.

(RMS 24617, Relator(a): CARLOS VELLOSO, Segunda Turma, julgado em 17/05/2005, DJ 10-06-2005 PP-00060 EMENT VOL-02195-02 PP-00266 RDDP n. 29, 2005, p. 209 RB v. 17, n. 500, 2005, p. 32-34 RDDP n. 30, 2005, p. 141-144 RTJ VOL-00194-02 PP-00582)

Link: **https://jurisprudencia.stf.jus.br/pages/search/sjur93569/false**

**CR 9854 AgR / UK - REINO UNIDO DA GRA-BRETANHA E DA IRLANDA DO NORTE**

CARTA ROGATÓRIA - COLABORAÇÃO - INEXISTÊNCIA DE TRATADO. A inexistência de tratado entre o país no qual situada a Justiça rogante e o Brasil não obstaculiza o cum-

primento de carta rogatória, implementando-se atos a partir do critério da cooperação internacional no combate ao crime.

CARTA ROGATÓRIA - OBJETO - DADOS DE PROCESSOS EM CURSO NO BRASIL E COLETA DE DEPOIMENTOS. O levantamento de dados constantes de processos em andamento no Brasil não implica a quebra do sigilo assegurado pela Carta da República, ante a publicidade que os reveste. No tocante à coleta de depoimentos, descabe examinar o envolvimento, ou não, no processo em curso no estrangeiro, daqueles que devem ser ouvidos, sob pena de mesclagem de jurisdições.

(CR 9854 AgR, Relator(a): MARCO AURÉLIO, Tribunal Pleno, julgado em 28/05/2003, DJ 27-06-2003 PP-00043 EMENT VOL-02116-02 PP-00393)

Link: **https://jurisprudencia.stf.jus.br/pages/search/sjur15008/false**

**HC 91867 / PA - PARÁ**

HABEAS CORPUS. NULIDADES: (1) INÉPCIA DA DENÚNCIA; (2) ILICITUDE DA PROVA PRODUZIDA DURANTE O INQUÉRITO POLICIAL; VIOLAÇÃO DE REGISTROS TELEFÔNICOS DO CORRÉU, EXECUTOR DO CRIME, SEM AUTORIZAÇÃO JUDICIAL; (3) ILICITUDE DA PROVA DAS INTERCEPTAÇÕES TELEFÔNICAS DE CONVERSAS DOS ACUSADOS COM ADVOGADOS, PORQUANTO ESSAS GRAVAÇÕES OFENDERIAM O DISPOSTO NO ART. 7º, II, DA LEI 8.906/96, QUE GARANTE O SIGILO DESSAS CONVERSAS. VÍCIOS NÃO CARACTERIZADOS. ORDEM DENEGADA.

1. Inépcia da denúncia. Improcedência. Preenchimento dos requisitos do art. 41 do CPP. A denúncia narra, de forma pormenorizada, os fatos e as circunstâncias. Pretensas omissões – nomes completos de outras vítimas, relacionadas a fatos que não constituem objeto da imputação – não importam em prejuízo à defesa.

2. Ilicitude da prova produzida durante o inquérito policial - violação de registros telefônicos de corréu, executor do crime, sem autorização judicial. 2.1 Suposta ilegalidade decorrente do fato de os policiais, após a prisão em flagrante do corréu, terem realizado a análise dos últimos registros telefônicos dos dois aparelhos celulares apreendidos. Não ocorrência. 2.2 Não se confundem comunicação telefônica e registros telefônicos, que recebem, inclusive, proteção jurídica distinta. Não se pode interpretar a cláusula do artigo 5º, XII, da CF, no sentido de proteção aos dados enquanto registro, depósito registral. A proteção constitucional é da comunicação de dados e não dos dados. 2.3 Art. 6º do CPP: dever da autoridade policial de proceder à coleta do material comprobatório da prática da infração penal. Ao proceder à pesquisa na agenda eletrônica dos aparelhos devidamente apreendidos, meio material indireto de prova, a autoridade policial, cumprindo o seu mister, buscou, unicamente, colher elementos de informação hábeis a esclarecer a autoria e a materialidade do delito (dessa análise logrou encontrar ligações entre o executor do homicídio e o ora paciente). Verificação que permitiu a orientação inicial da linha investigatória a ser adotada, bem como possibilitou concluir que os aparelhos seriam relevantes para a investigação. 2.4 À guisa de mera argumentação, mesmo que se pudesse reputar a prova produzida como ilícita e as demais, ilícitas por derivação, nos termos da teoria dos frutos da árvore venenosa (fruit of the poisonous tree), é certo que, ainda assim, melhor sorte não assistiria à defesa. É que, na hipótese, não há que se falar em prova ilícita por derivação. Nos termos da teoria da descoberta inevitável, construída pela Suprema Corte norte-americana no caso Nix x Williams (1984), o curso normal das investigações conduziria a elementos informativos que vinculariam os pacientes ao fato investigado. Bases desse entendimento que parecem ter encontrado guarida no ordenamento jurídico pátrio com o advento da Lei 11.690/2008, que deu nova redação ao art. 157 do CPP, em especial o seu § 2º.

3. Ilicitude da prova das interceptações telefônicas de conversas dos acusados com advogados, ao argumento de que essas gravações ofenderiam o disposto no art. 7º, II, da Lei n. 8.906/96, que garante o sigilo dessas conversas. 3.1 Nos termos do art. 7º, II, da Lei 8.906/94, o Estatuto da Advocacia garante ao advogado a inviolabilidade de seu escritório ou local de trabalho, bem como de seus instrumentos de trabalho, de sua correspondência escrita, eletrônica, telefônica e telemática, desde que relativas ao exercício da advocacia. 3.2 Na hipótese, o magistrado de primeiro grau, por reputar necessária a realização da prova, determinou, de forma fundamentada, a interceptação telefônica direcionada às pessoas investigadas, não tendo, em momento algum, ordenado a devassa das linhas telefônicas dos advogados dos pacientes. Mitigação que

pode, eventualmente, burlar a proteção jurídica. 3.3 Sucede que, no curso da execução da medida, os diálogos travados entre o paciente e o advogado do corréu acabaram, de maneira automática, interceptados, aliás, como qualquer outra conversa direcionada ao ramal do paciente. Inexistência, no caso, de relação jurídica cliente-advogado. 3.4 Não cabe aos policiais executores da medida proceder a uma espécie de filtragem das escutas interceptadas. A impossibilidade desse filtro atua, inclusive, como verdadeira garantia ao cidadão, porquanto retira da esfera de arbítrio da polícia escolher o que é ou não conveniente ser interceptado e gravado. Valoração, e eventual exclusão, que cabe ao magistrado a quem a prova é dirigida.

4. Ordem denegada.

(HC 91867, Relator(a): GILMAR MENDES, Segunda Turma, julgado em 24/04/2012, ACÓRDÃO ELETRÔNICO DJe-185 DIVULG 19-09-2012 PUBLIC 20-09-2012)

Este texto não substitui a publicação oficial.

Link: **https://jurisprudencia.stf.jus.br/pages/search/sjur214794/false**

**MS 33340 / DF - DISTRITO FEDERAL**

Ementa: DIREITO ADMINISTRATIVO. CONTROLE LEGISLATIVO FINANCEIRO. CONTROLE EXTERNO. REQUISIÇÃO PELO TRIBUNAL DE CONTAS DA UNIÃO DE INFORMAÇÕES ALUSIVAS A OPERAÇÕES FINANCEIRAS REALIZADAS PELAS IMPETRANTES. RECUSA INJUSTIFICADA. DADOS NÃO ACOBERTADOS PELO SIGILO BANCÁRIO E EMPRESARIAL.

1. O controle financeiro das verbas públicas é essencial e privativo do Parlamento como consectário do Estado de Direito (IPSEN, Jörn. Staatsorganisationsrecht. 9. Auflage. Berlin: Luchterhand, 1997, p. 221).

2. O primado do ordenamento constitucional democrático assentado no Estado de Direito pressupõe uma transparente responsabilidade do Estado e, em especial, do Governo. (BADURA, Peter. Verfassung, Staat und Gesellschaft in der Sicht des Bundesverfassungsgerichts. In: Bundesverfassungsgericht und Grundgesetz. Festgabe aus Anlass des 25jähringe Bestehens des Bundesverfassungsgerichts. Weiter Band. Tübingen: Mohr, 1976, p. 17.)



3. O sigilo de informações necessárias para a preservação da intimidade é relativizado quando se está diante do interesse da sociedade de se conhecer o destino dos recursos públicos.

4. Operações financeiras que envolvam recursos públicos não estão abrangidas pelo sigilo bancário a que alude a Lei Complementar nº 105/2001, visto que as operações dessa espécie estão submetidas aos princípios da administração pública insculpidos no art. 37 da Constituição Federal. Em tais situações, é prerrogativa constitucional do Tribunal [TCU] o acesso a informações relacionadas a operações financiadas com recursos públicos.

5. O segredo como "alma do negócio" consubstancia a máxima cotidiana inaplicável em casos análogos ao sub judice, tanto mais que, quem contrata com o poder público não pode ter segredos, especialmente se a revelação for necessária para o controle da legitimidade do emprego dos recursos públicos. É que a contratação pública não pode ser feita em esconderijos envernizados por um arcabouço jurídico capaz de impedir o controle social quanto ao emprego das verbas públicas.

6. "O dever administrativo de manter plena transparência em seus comportamentos impõe não haver em um Estado Democrático de Direito, no qual o poder reside no povo (art. 1º, parágrafo único, da Constituição), ocultamento aos administrados dos assuntos que a todos interessam, e muito menos em relação aos sujeitos individualmente afetados por alguma medida." (MELLO, Celso Antônio Bandeira de. Curso de Direito Administrativo. 27ª edição. São Paulo: Malheiros, 2010, p. 114).

7. O Tribunal de Contas da União não está autorizado a, manu militari, decretar a quebra de sigilo bancário e empresarial de terceiros, medida cautelar condicionada à prévia anuência do Poder Judiciário, ou, em situações pontuais, do Poder Legislativo. Precedente: MS 22.801, Tribunal Pleno, Rel. Min. Menezes Direito, DJe 14.3.2008.

8. In casu, contudo, o TCU deve ter livre acesso às operações financeiras realizadas pelas impetrantes, entidades de direito privado da Administração Indireta submetidas ao seu controle financeiro, mormente porquanto operacionalizadas mediante o emprego

de recursos de origem pública. Inoponibilidade de sigilo bancário e empresarial ao TCU quando se está diante de operações fundadas em recursos de origem pública. Conclusão decorrente do dever de atuação transparente dos administradores públicos em um Estado Democrático de Direito.

9. A preservação, in casu, do sigilo das operações realizadas pelo BNDES e BNDESPAR com terceiros não, apenas, impediria a atuação constitucionalmente prevista para o TCU, como, também, representaria uma acanhada, insuficiente, e, por isso mesmo, desproporcional limitação ao direito fundamental de preservação da intimidade.

10. O princípio da conformidade funcional a que se refere Canotilho, também, reforça a conclusão de que os órgãos criados pela Constituição da República, tal como o TCU, devem se manter no quadro normativo de suas competências, sem que tenham autonomia para abrir mão daquilo que o constituinte lhe entregou em termos de competências. (CANOTILHO, José Joaquim Gomes. Direito Constitucional e Teoria da Constituição. 5ª edição. Coimbra: Almedina, 2002, p. 541.)

11. A Proteção Deficiente de vedação implícita permite assentar que se a publicidade não pode ir tão longe, de forma a esvaziar, desproporcionalmente, o direito fundamental à privacidade e ao sigilo bancário e empresarial; não menos verdadeiro é que a insuficiente limitação ao direito à privacidade revelar-se-ia, por outro ângulo, desproporcional, porquanto lesiva aos interesses da sociedade de exigir do Estado brasileiro uma atuação transparente.

12. No caso sub examine: I) O TCU determinou o fornecimento de dados pela JBS/Friboi, pessoa que celebrou contratos vultosos com o BNDES, a fim de aferir, por exemplo, os critérios utilizados para a escolha da referida sociedade empresária, quais seriam as vantagens sociais advindas das operações analisadas, se houve cumprimento das cláusulas contratuais, se as operações de troca de debêntures por posição acionária na empresa ora indicada originou prejuízo para o BNDES. II) O TCU não agiu de forma imotivada e arbitrária, e nem mesmo criou exigência irrestrita e genérica de informações sigilosas. Sobre o tema, o ato coator aponta a existência de uma operação da Polícia Federal denominada Operação Santa Tereza que apontou a existência de quadrilha intermediando empréstimos junto ao BNDES, inclusive envolvendo o financiamento obtido



pelo Frigorífico Friboi. Ademais, a necessidade do controle financeiro mais detido resultou, segundo o decisum atacado, de um "protesto da Associação Brasileira da Indústria Frigorífica (Abrafigo) contra a política do BNDES que estava levanto à concentração econômica do setor". III) A requisição feita pelo TCU na hipótese destes autos revela plena compatibilidade com as atribuições constitucionais que lhes são dispensadas e permite, de forma idônea, que a sociedade brasileira tenha conhecimento se os recursos públicos repassados pela União ao seu banco de fomento estão sendo devidamente empregados.

13. Consequentemente a recusa do fornecimento das informações restou inadmissível, porquanto imprescindíveis para o controle da sociedade quanto à destinação de vultosos recursos públicos. O que revela que o determinado pelo TCU não extrapola a medida do razoável.

14. Merece destacar que in casu: a) Os Impetrantes são bancos de fomento econômico e social, e não instituições financeiras privadas comuns, o que impõe, aos que com eles contratam, a exigência de disclosure e de transparência, valores a serem prestigiados em nossa República contemporânea, de modo a viabilizar o pleno controle de legitimidade e responsividade dos que exercem o poder. b) A utilização de recursos públicos por quem está submetido ao controle financeiro externo inibe a alegação de sigilo de dados e autoriza a divulgação das informações necessárias para o controle dos administradores, sob pena de restar inviabilizada a missão constitucional da Corte de Contas. c) À semelhança do que já ocorre com a CVM e com o BACEN, que recebem regularmente dados dos Impetrantes sobre suas operações financeiras, os Demandantes, também, não podem se negar a fornecer as informações que forem requisitadas pelo TCU.

15. A limitação ao direito fundamental à privacidade que, por se revelar proporcional, é compatível com a teoria das restrições das restrições (Schranken-Schranken). O direito ao sigilo bancário e empresarial, mercê de seu caráter fundamental, comporta uma proporcional limitação destinada a permitir o controle financeiro da Administração Publica por órgão constitucionalmente previsto e dotado de capacidade institucional para tanto.

16. É cediço na jurisprudência do E. STF que: "ADMINISTRAÇÃO PÚBLICA – PUBLICIDADE. A transparência decorre do princípio da publicidade. TRIBUNAL DE CONTAS

– FISCALIZAÇÃO – DOCUMENTOS. Descabe negar ao Tribunal de Contas o acesso a documentos relativos à Administração Pública e ações implementadas, não prevalecendo a óptica de tratar-se de matérias relevantes cuja divulgação possa importar em danos para o Estado. Inconstitucionalidade de preceito da Lei Orgânica do Tribunal de Contas do Estado do Ceará que implica óbice ao acesso." (ADI 2.361, Tribunal Pleno, Rel. Min. Marco Aurélio, DJe 23/10/2014).

17. Jusfilosoficamente as premissas metodológicas aplicáveis ao caso sub judice revelam que: I - "nuclearmente feito nas pranchetas da Constituição. Foi o legislador de primeiríssimo escalão quem estruturou e funcionalizou todos eles (os Tribunais de Contas), prescindindo das achegas da lei menor. (...) Tão elevado prestígio conferido ao controle externo e a quem dele mais se ocupa, funcionalmente, é reflexo direto do princípio republicano. Pois, numa República, impõe-se responsabilidade jurídica pessoal a todo aquele que tenha por competência (e consequente dever) cuidar de tudo que é de todos". (BRITTO, Carlos Ayres. O regime constitucional dos Tribunais de Contas. In: Revista do Tribunal de Contas do Estado do Rio de Janeiro. Volume 8. 2º semestre de 2014. Rio de Janeiro: TCE-RJ, p. 18 e 20) II - "A legitimidade do Estado Democrático de Direito depende do controle da legitimidade da sua ordem financeira. Só o controle rápido, eficiente, seguro, transparente e valorativo dos gastos públicos legitima o tributo, que é o preço da liberdade. O aperfeiçoamento d controle é que pode derrotar a moral tributária cínica, que prega a sonegação e a desobediência civil a pretexto da ilegitimidade da despesa pública. (TORRES, Ricardo Lobo. Uma Avaliação das Tendências Contemporâneas do Direito Administrativo. Obra em homenagem a Eduardo García de Enterría. Rio de Janeiro: Renovar, 2003, p. 645)

18. Denegação da segurança por ausência de direito material de recusa da remessa dos documentos.

(MS 33340, Relator(a): LUIZ FUX, Primeira Turma, julgado em 26/05/2015, PROCESSO ELETRÔNICO DJe-151 DIVULG 31-07-2015 PUBLIC 03-08-2015)

Link: **https://jurisprudencia.stf.jus.br/pages/search/sjur313576/false**



**Rcl 9428 / DF - DISTRITO FEDERAL**

EMENTA: LIBERDADE DE IMPRENSA. Decisão liminar. Proibição de reprodução de dados relativos ao autor de ação inibitória ajuizada contra empresa jornalística. Ato decisório fundado na expressa invocação da inviolabilidade constitucional de direitos da personalidade, notadamente o da privacidade, mediante proteção de sigilo legal de dados cobertos por segredo de justiça. Contraste teórico entre liberdade de imprensa e os direitos previstos nos arts. 5º, incs. X e XII, e 220, caput, da CF. Ofensa à autoridade do acórdão proferido na ADPF nº 130, que deu por não recebida a Lei de Imprensa. Não ocorrência. Matéria não decidida na ADPF. Processo de reclamação extinto, sem julgamento de mérito. Votos vencidos. Não ofende a autoridade do acórdão proferido na ADPF nº 130, a decisão que, proibindo a jornal a publicação de fatos relativos ao autor de ação inibitória, se fundou, de maneira expressa, na inviolabilidade constitucional de direitos da personalidade, notadamente o da privacidade, mediante proteção de sigilo legal de dados cobertos por segredo de justiça.

(Rcl 9428, Relator(a): CEZAR PELUSO, Tribunal Pleno, julgado em 10/12/2009, DJe-116 DIVULG 24-06-2010 PUBLIC 25-06-2010 EMENT VOL-02407-01 PP-00175 RTJ VOL-00216-01 PP-00279)

Link: **https://jurisprudencia.stf.jus.br/pages/search/sjur179885/false**

**PPE 732 QO / DF - DISTRITO FEDERAL**

E M E N T A: EXTRADIÇÃO – PRISÃO CAUTELAR – PLEITO FORMULADO PELA INTERPOL – POSSIBILIDADE – INOVAÇ ÃO INTRODUZIDA PELA LEI Nº 12.878/2013 – DELITO INFORMÁTICO (CRIME DIGITAL): "INVASÃO DE DISPOSITIVO INFORMÁTICO" (CP, ART. 154-A, ACRESCIDO PELA LEI Nº 12.737/2012) – FATO DELITUOSO ALEGADAMENTE COMETIDO, EM TERRITÓRIO AMERICANO (ESTADO DO TEXAS), EM 2011 – CONDUTA QUE, NO MOMENTO EM QUE PRATICADA (2011), AINDA NÃO SE REVESTIA DE TIPICIDADE PENAL NO ORDENAMENTO POSITIVO BRASILEIRO – O SIGNIFICADO JURÍDICO DO PRINCÍPIO CONSTITUCIONAL DA RESERVA DE LEI EM MATÉRIA DE TIPIFICAÇÃO E DE COMINAÇÃO PENAIS (CF, ART. 5º, INCISO XXXIX) – "NULLUM CRIMEN, NULLA POE-

NA SINE PRAEVIA LEGE" – DUPLA TIPICIDADE (OU DUPLA INCRIMINAÇÃO): CRITÉRIO QUE REGE O SISTEMA EXTRADICIONAL – NECESSIDADE DE QUE O FATO SUBJACENTE AO PEDIDO DE EXTRADIÇÃO (OU AO PLEITO DE PRISÃO CAUTELAR PARA EFEITOS EXTRADICIONAIS) ESTEJA SIMULTANEAMENTE TIPIFICADO, NO MOMENTO DE SUA PRÁTICA, TANTO NA LEGISLAÇÃO PENAL DO BRASIL QUANTO NA DO ESTADO ESTRANGEIRO – PRECEDENTES – SITUAÇÃO INOCORRENTE NO CASO, POIS A CONDUTA PUNÍVEL IMPUTADA AO SÚDITO ESTRANGEIRO RECLAMADO SOMENTE PASSOU A SER CONSIDERADA CRIMINOSA, NO BRASIL, EM ABRIL DE 2013 (QUANDO SE ESGOTOU O PERÍODO DE "VACATIO LEGIS" DA LEI Nº 12.737/2012, ART. 4º), POSTERIORMENTE, PORTANTO, À DATA EM QUE FOI ELA ALEGADAMENTE PRATICADA NOS ESTADOS UNIDOS DA AMÉRICA – EVOLUÇÃO DO TRATAMENTO LEGISLATIVO, NO BRASIL, PARA FINS PENAIS, DOS CRIMES INFORMÁTICOS – OCORRÊNCIA, AINDA, NA ESPÉCIE, DE OUTRO OBSTÁCULO JURÍDICO: DELITO INFORMÁTICO (OU CRIME DIGITAL, OU INFRAÇÃO PENAL CIBERNÉTICA) SEQUER PREVISTO NO ARTIGO II DO TRATADO DE EXTRADIÇÃO BRASIL/EUA – ROL EXAUSTIVO, FUNDADO EM "NUMERUS CLAUSUS", QUE DEFINE, NO CONTEXTO BILATERAL DAS RELAÇÕES EXTRADICIONAIS ENTRE BRASIL E EUA, OS CRIMES QUALIFICADOS PELA NOTA DE "EXTRADITABILIDADE" – PRECEDENTES, A ESSE RESPEITO, DO SUPREMO TRIBUNAL FEDERAL – CONSEQUENTE IMPOSSIBILIDADE DE PROCESSAR-SE DEMANDA EXTRADICIONAL FUNDADA EM DELITO ESTRANHO AO ROL TAXATIVO INSCRITO NO ARTIGO II DESSE TRATADO DE EXTRADIÇÃO – NATUREZA JURÍDICA DO TRATADO DE EXTRADIÇÃO ("LEX SPECIALIS") – PRECEDÊNCIA JURÍDICA, QUANTO À SUA APLICABILIDADE, SOBRE O ORDENAMENTO POSITIVO INTERNO DO BRASIL – "PACTA SUNT SERVANDA" – PRECEDENTES – A INADMISSIBILIDADE DA EXTRADIÇÃO (CAUSA PRINCIPAL) TORNA INVIÁVEL O ATENDIMENTO DO PEDIDO DE PRISÃO PREVENTIVA (MEDIDA REVESTIDA DE CAUTELARIDADE E IMPREGNADA DE CARÁTER ANCILAR E MERAMENTE ACESSÓRIO) – QUESTÃO DE ORDEM QUE SE RESOLVE NO SENTIDO DO INDEFERIMENTO DO PEDIDO DE PRISÃO CAUTELAR. (PPE 732 QO, Relator(a): CELSO DE MELLO, Segunda Turma, julgado em 11/11/2014, ACÓRDÃO ELETRÔNICO DJe-021 DIVULG 30-01-2015 PUBLIC 02-02-2015)

Link: **https://jurisprudencia.stf.jus.br/pages/search/sjur290508/false**



**ADI 2859 / DF - DISTRITO FEDERAL**

EMENTA Ação direta de inconstitucionalidade. Julgamento conjunto das ADI nº 2.390, 2.386, 2.397 e 2.859. Normas federais relativas ao sigilo das operações de instituições financeiras. Decreto nº 4.545/2002. Exaurimento da eficácia. Perda parcial do objeto da ação direta nº 2.859. Expressão "do inquérito ou", constante no § 4º do art. 1º, da Lei Complementar nº 105/2001. Acesso ao sigilo bancário nos autos do inquérito policial. Possibilidade. Precedentes. Art. 5º e 6º da Lei Complementar nº 105/2001 e seus decretos regulamentadores. Ausência de quebra de sigilo e de ofensa a direito fundamental. Confluência entre os deveres do contribuinte (o dever fundamental de pagar tributos) e os deveres do Fisco (o dever de bem tributar e fiscalizar). Compromissos internacionais assumidos pelo Brasil em matéria de compartilhamento de informações bancárias. Art. 1º da Lei Complementar nº 104/2001. Ausência de quebra de sigilo. Art. 3º, § 3º, da LC 105/2001. Informações necessárias à defesa judicial da atuação do Fisco. Constitucionalidade dos preceitos impugnados. ADI nº 2.859. Ação que se conhece em parte e, na parte conhecida, é julgada improcedente. ADI nº 2.390, 2.386, 2.397. Ações conhecidas e julgadas improcedentes.

1. Julgamento conjunto das ADI nº 2.390, 2.386, 2.397 e 2.859, que têm como núcleo comum de impugnação normas relativas ao fornecimento, pelas instituições financeiras, de informações bancárias de contribuintes à administração tributária.

2. Encontra-se exaurida a eficácia jurídico-normativa do Decreto nº 4.545/2002, visto que a Lei n º 9.311, de 24 de outubro de 1996, de que trata este decreto e que instituiu a CPMF, não está mais em vigência desde janeiro de 2008, conforme se depreende do art. 90, § 1º, do Ato das Disposições Constitucionais Transitórias -ADCT. Por essa razão, houve parcial perda de objeto da ADI nº 2.859/DF, restando o pedido desta ação parcialmente prejudicado. Precedentes.

3. A expressão "do inquérito ou", constante do § 4º do art. 1º da Lei Complementar nº 105/2001, refere-se à investigação criminal levada a efeito no inquérito policial, em cujo âmbito esta Suprema Corte admite o acesso ao sigilo bancário do investigado, quando presentes indícios de prática criminosa. Precedentes: AC 3.872/DF-AgR, Relator o Mi-

nistro Teori Zavascki, Tribunal Pleno, DJe de 13/11/15; HC 125.585/PE-AgR, Relatora a Ministra Cármen Lúcia, Segunda Turma, DJe de 19/12/14; Inq 897-AgR, Relator o Ministro Francisco Rezek, Tribunal Pleno, DJ de 24/3/95.

4. Os artigos 5º e 6º da Lei Complementar nº 105/2001 e seus decretos regulamentares (Decretos nº 3.724, de 10 de janeiro de 2001, e nº 4.489, de 28 de novembro de 2009) consagram, de modo expresso, a permanência do sigilo das informações bancárias obtidas com espeque em seus comandos, não havendo neles autorização para a exposição ou circulação daqueles dados. Trata-se de uma transferência de dados sigilosos de um determinado portador, que tem o dever de sigilo, para outro, que mantém a obrigação de sigilo, permanecendo resguardadas a intimidade e a vida privada do correntista, exatamente como determina o art. 145, § 1º, da Constituição Federal.

5. A ordem constitucional instaurada em 1988 estabeleceu, dentre os objetivos da República Federativa do Brasil, a construção de uma sociedade livre, justa e solidária, a erradicação da pobreza e a marginalização e a redução das desigualdades sociais e regionais. Para tanto, a Carta foi generosa na previsão de direitos individuais, sociais, econômicos e culturais para o cidadão. Ocorre que, correlatos a esses direitos, existem também deveres, cujo atendimento é, também, condição sine qua non para a realização do projeto de sociedade esculpido na Carta Federal. Dentre esses deveres, consta o dever fundamental de pagar tributos, visto que são eles que, majoritariamente, financiam as ações estatais voltadas à concretização dos direitos do cidadão. Nesse quadro, é preciso que se adotem mecanismos efetivos de combate à sonegação fiscal, sendo o instrumento fiscalizatório instituído nos arts. 5º e 6º da Lei Complementar nº 105/ 2001 de extrema significância nessa tarefa.

6. O Brasil se comprometeu, perante o G20 e o Fórum Global sobre Transparência e Intercâmbio de Informações para Fins Tributários (Global Forum on Transparency and Exchange of Information for Tax Purposes), a cumprir os padrões internacionais de transparência e de troca de informações bancárias, estabelecidos com o fito de evitar o descumprimento de normas tributárias, assim como combater práticas criminosas. Não deve o Estado brasileiro prescindir do acesso automático aos dados bancários dos contribuintes por sua administração tributária, sob pena de descumprimento de seus compromissos internacionais.

7. O art. 1º da Lei Complementar 104/2001, no ponto em que insere o § 1º, inciso II, e o § 2º ao art. 198 do CTN, não determina quebra de sigilo, mas transferência de informações sigilosas no âmbito da Administração Pública. Outrossim, a previsão vai ao encontro de outros comandos legais já amplamente consolidados em nosso ordenamento jurídico que permitem o acesso da Administração Pública à relação de bens, renda e patrimônio de determinados indivíduos.

8. À Procuradoria-Geral da Fazenda Nacional, órgão da Advocacia-Geral da União, caberá a defesa da atuação do Fisco em âmbito judicial, sendo, para tanto, necessário o conhecimento dos dados e informações embasadores do ato por ela defendido. Resulta, portanto, legítima a previsão constante do art. 3º, § 3º, da LC 105/2001.

9. Ação direta de inconstitucionalidade nº 2.859/DF conhecida parcialmente e, na parte conhecida, julgada improcedente. Ações diretas de inconstitucionalidade nº 2390, 2397, e 2386 conhecidas e julgadas improcedentes. Ressalva em relação aos Estados e Municípios, que somente poderão obter as informações de que trata o art. 6º da Lei Complementar nº 105/2001 quando a matéria estiver devidamente regulamentada, de maneira análoga ao Decreto federal nº 3.724/2001, de modo a resguardar as garantias processuais do contribuinte, na forma preconizada pela Lei nº 9.784/99, e o sigilo dos seus dados bancários.

(ADI 2859, Relator(a): DIAS TOFFOLI, Tribunal Pleno, julgado em 24/02/2016, ACÓRDÃO ELETRÔNICO DJe-225 DIVULG 20-10-2016 PUBLIC 21-10-2016)

Link: **https://jurisprudencia.stf.jus.br/pages/search/sjur358417/false**

**ADI 6387 MC / DF - DISTRITO FEDERAL**

Decisão: MEDIDA CAUTELAR DE URGÊNCIA Vistos etc.

1. Cuida-se de pedido de medida cautelar em ação direta de inconstitucionalidade proposta pelo Conselho Federal da Ordem dos Advogados do Brasil – CFOAB contra

o inteiro teor da Medida Provisória n. 954, de 17 de abril de 2020, que dispõe sobre "o compartilhamento de dados por empresas de telecomunicações prestadoras de Serviço Telefônico Fixo Comutado e de Serviço Móvel Pessoal com a Fundação Instituto Brasileiro de Geografia e Estatística, para fins de suporte à produção estatística oficial durante a situação de emergência de saúde pública de importância internacional decorrente do coronavírus (covid19), de que trata a Lei nº 13.979, de 6 de fevereiro de 2020".

2. Para a adequada compreensão da controvérsia constitucional, transcrevo o inteiro teor do ato normativo questionado: Art. 1º Esta Medida Provisória dispõe sobre o compartilhamento de dados por empresas de telecomunicações prestadoras do Serviço Telefônico Fixo Comutado - STFC e do Serviço Móvel Pessoal - SMP com a Fundação Instituto Brasileiro de Geografia e Estatística - IBGE. Parágrafo único. O disposto nesta Medida Provisória se aplica durante a situação de emergência de saúde pública de importância internacional decorrente do coronavírus (covid19), de que trata a Lei nº 13.979, de 6 de fevereiro de 2020. Art. 2º As empresas de telecomunicação prestadoras do STFC e do SMP deverão disponibilizar à Fundação IBGE, em meio eletrônico, a relação dos nomes, dos números de telefone e dos endereços de seus consumidores, pessoas físicas ou jurídicas. § 1º Os dados de que trata o caput serão utilizados direta e exclusivamente pela Fundação IBGE para a produção estatística oficial, com o objetivo de realizar entrevistas em caráter não presencial no âmbito de pesquisas domiciliares. § 2º Ato do Presidente da Fundação IBGE, ouvida a Agência Nacional de Telecomunicações, disporá, no prazo de três dias, contado da data de publicação desta Medida Provisória, sobre o procedimento para a disponibilização dos dados de que trata o caput. § 3º Os dados deverão ser disponibilizados no prazo de: I - sete dias, contado da data de publicação do ato de que trata o § 2º; e II - quatorze dias, contado da data da solicitação, para as solicitações subsequentes. Art. 3º Os dados compartilhados: I - terão caráter sigiloso; II - serão usados exclusivamente para a finalidade prevista no § 1º do art. 2º; e III - não serão utilizados como objeto de certidão ou meio de prova em processo administrativo, fiscal ou judicial, nos termos do disposto na Lei nº 5.534, de 14 de novembro de 1968. § 1º É vedado à Fundação IBGE disponibilizar os dados a que se refere o caput do art. 2º a quaisquer empresas públicas ou privadas ou a órgãos ou entidades da administração pública direta ou indireta de quaisquer dos entes federativos. § 2º A Fundação IBGE informará, em seu sítio eletrônico, as situações em que os dados referidos no caput do art. 2º foram utilizados e divulgará relatório de impacto à proteção de dados pessoais, nos termos do disposto na Lei nº 13.709, de 14 de agosto de 2018. Art. 4º Superada a situação de emergência de saúde pública de importância internacional decorrente do coronavírus (covid-19), nos termos do disposto na Lei nº 13.979, de 2020, as informações compartilhadas na forma prevista no caput do art. 2º ou no art. 3º serão eliminadas das bases de dados da Fundação IBGE. Parágrafo único. Na hipótese de necessidade de conclusão de produção estatística oficial, a Fundação IBGE poderá utilizar os dados pelo prazo de trinta dias, contado do fim da situação de emergência de saúde pública de importância internacional. Art. 5º Esta Medida Provisória entra em vigor na data de sua publicação. Brasília, 17 de abril de 2020; 199º da Independência e 132º da República."

3. A parte autora afirma presentes os vícios da inconstitucionalidade formal, por inobservância dos requisitos constitucionais para edição de medida provisória, e da inconstitucionalidade material, ao argumento principal de violação das regras constitucionais da dignidade da pessoa humana, da inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas, do sigilo dos dados e da autodeterminação informativa (arts. 1º, III e 5º, X e XII, da Constituição da República).

4. Conforme assinala, a inconstitucionalidade formal diz com a inobservância do art. 62, caput, da Constituição Federal, na medida em que não demonstrados os requisitos da urgência e da relevância material a autorizar a edição de medida provisória. À alegação da inconstitucionalidade formal, defende a possibilidade de sindicância jurisdicional, a despeito da jurisprudência construída, no período do regime militar, no sentido de sua inviabilidade quanto a atos de natureza política. Nesse sentido, reporta-se à ADI-MC 162, à ADI 2213 e à ADI 4029, em que reformulado o fundamento da legitimidade de controle constitucional dos pressupostos do exercício do poder extraordinário de legislar outorgado ao Presidente da República como instrumento de tutela do preceito fundamental da separação de poderes. Segundo argui, a MP n. 954/2020 não evidencia a importância superlativa da pesquisa estatística que embasa a solicitação de compartilhamento dos dados, tampouco

explicita a forma como esta pesquisa contribuirá na formulação das políticas públicas de enfrentamento da crise sanitária, uma vez não informados os tipos de pesquisas a serem realizadas. Noutro espectro, destaca não esclarecido o motivo para o compartilhamento de dados, já informado pelo IBGE o adiamento do Censo Demográfico para o ano de 2021.

5. Busca seja assentada a inconstitucionalidade material da MP n. 954/2020. Para tanto, assevera a necessidade de tutela do direito fundamental à proteção de dados pessoais, a teor do art. 5º, XII, da CF, que assegura a inviolabilidade do sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, ressalvada a relativização, nessa última hipótese, mediante ordem judicial e para fins de persecução penal. Argumenta com o direito fundamental à inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas (art. 5º, X, CF), como fundamento do indivíduo para determinar e controlar, frente ao Estado, a utilização dos seus dados. Seguindo essa linha discursiva, aponta para a existência, no desenho constitucional brasileiro, de um direito fundamental à proteção de dados, na concepção de um direito à autodeterminação informativa, em que fundamenta, inclusive, a edição da Lei Geral de Proteção de Dados (Lei n. 13.709/2018). Ainda nessa perspectiva e para ilustrar, invoca a decisão do Tribunal Constitucional Federal Alemão que reconheceu, em 1983, forte no direito geral da personalidade, o direito fundamental à autodeterminação sobre dados pessoais, diante de intervenções estatais. Conforme argumenta "a autodeterminação individual pressupõe – mesmo sob as condições da moderna tecnologia de processamento de informação – que, ao indivíduo está garantida a liberdade de decisão sobre as ações a serem procedidas ou omitidas e, inclusive, a possibilidade de se comportar realmente conforme tal decisão". Alega necessária, no ponto, a explicitação do postulado da proporcionalidade para as hipóteses de relativização do afirmado direito fundamental à autodeterminação informativa. Ou seja, articula que a atividade legislativa será constitucional se observar a proporcionalidade nos critérios a embasar a intervenção estatal na coleta, no compartilhamento e no uso dos dados pessoais, conduta não adotada no ato normativo contestado. Isso porque a MP n. 954/2020 não explicita a finalidade do uso da pesquisa estatística, não demonstra a forma pela qual adequados e necessários os dados nem delimita o campo de proteção na operação de processamento de dados.



Importa registrar a indicação do precedente formado no RE 1055941, sobre o compartilhamento de dado pelo COAF/UIF ao Ministério Público. Em suas palavras: "A Medida Provisória em análise viola o sigilo de dados dos brasileiros e invade a privacidade e a intimidade de todos, sem a devida proteção quanto à segurança de manuseio, sem justificativa adequada, sem finalidade suficientemente especificada e sem garantir a manutenção do sigilo por uma Autoridade com credibilidade, representatividade e legitimidade, a exemplo daquela prevista pela Lei Geral de Proteção de Dados, Lei Federal 13.709."

6. Frente ao cenário argumentativo descrito, requer a concessão de medida cautelar, ad referendum do Plenário, na forma do art. 10, § 3º, da Lei nº 9.868/1999, para suspender imediatamente a eficácia do inteiro teor da MP n. 954/2020 até o julgamento final da presente ação, bem como para reconhecer o "direito fundamental à autodeterminação informativa, a ensejar tutela jurisdicional quando sua violação não for devidamente justificada por motivo suficiente, proporcional, necessário e adequado e com proteção efetiva do sigilo perante terceiros, com governança que inclua o Judiciário, o Ministério Público, a Advocacia e entidades da sociedade civil".

7. Justifica presente o requisito da plausibilidade do direito, à evidência da não configuração dos requisitos constitucionais autorizadores da edição de medidas provisórias (art. 62, caput, CF), e da necessidade de tutela dos direitos fundamentais à privacidade, à intimidade, à proteção de dados pessoais, à dignidade da pessoa humana e à autodeterminação informativa. Igualmente, destaca configurado o perigo da demora na prestação jurisdicional face à urgência reconhecida no exíguo prazo de três dias estipulado no art. 2º, §2º, da MP n. 954/2020 para a disciplina do procedimento de disponibilização de dados, a partir da oitiva da Agência Nacional de Telecomunicações. Após a regulamentação, abre-se o prazo de sete dias para as empresas oferecerem os dados solicitados. Afirma, portanto, "no mais tardar, dia  27 próximo todos os dados dos brasileiros já deverão estar disponibilizados, nos termos da MP".

8. No mérito, pede a procedência do pedido de declaração de inconstitucionalidade da Medida Provisória n. 954/2020, em sua integralidade, bem como o reconhecimento do direito fundamental à autodeterminação informativa.

9. Considerada a relevância da matéria constitucional objeto da ação, bem como a urgência caracterizada da tutela jurisdicional, solicitei informações prévias à Fundação Instituto Brasileiro de Geografia e Estatística - IBGE e à Agência Nacional de Telecomunicações - ANATEL, bem como abri vista para manifestação do Procurador-Geral da República e do Advogado-Geral da União, no prazo comum de 48 (quarenta e oito) horas.

10. Em 23.4.2020, o autor peticionou informando que no curso do prazo de 48 (quarenta e oito) horas concedido para a juntada das informações, foi publicada , em 22.4.2020, a "Instrução Normativa IBGE 2/2020, que regula de maneira genérica e precária o procedimento de compartilhamento direto de dados, sob responsabilidade de sua Diretoria de Informática" (doc. n. 24867/2020). Nas suas palavras, conforme o ofício anexo, "devidamente desidentificado pela remetente para não apresentar informações sensíveis, o IBGE já começou a oficiar as operadoras de telefonia móvel e fixa para que enviem os dados pessoais sob sua guarda à fundação pública."

11. À alegação de que algumas operadoras de telefonia já receberam o ofício encaminhado pelo IBGE, com fundamento na Instrução Normativa 2/2020, para a transferência imediata dos dados, a despeito do prazo de sete dias fixados pela Medida Provisória n. 954/2020, e o prazo de 48 horas fixado por este Supremo Tribunal Federal, reitera o pedido de urgência a justificar a medida liminar requerida.

12. Em 24.4.2020, o Advogado-Geral da União manifestou-se pelo indeferimento da medida cautelar, em arrazoado assim ementado: "Medida Provisória nº 954/2020. Compartilhamento de dados por empresas de telecomunicações com a Fundação IBGE. Legitimidade formal. A relevância e a urgência da medida encontram fundamento na necessidade de permitir, em contexto de distanciamento social, a continuidade e o enriquecimento do diagnóstico estatístico oferecido pelo IBGE. Conhecimento relevante para a formulação cientificamente adequada de políticas públicas de combate às consequências do Covid-19. Legitimidade material. Ausência de fumus boni iuris. Ausência de violação à privacidade e à intimidade (artigo 5º, incisos X e XII, da Constituição da República). Essa Suprema Corte já decidiu que a 'transferência de dados sigilosos de um determinado portador, que tem o dever de sigilo, para outro, que mantém a obrigação de sigilo' não ofende o direito à intimidade e à privacidade. ADI nº 2859. O acesso aos dados pessoais na forma da MP nº 954/2020 contempla finalidade (pesquisa estatística) e condicionantes consentâneos com a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018). Obrigação de conservação do sigilo e posterior eliminação dos dados coletados. Indispensabilidade do prosseguimento do levantamento estatístico da PNAD. Subsídios necessários, entre outros fins, para servir de base ao cálculo do Fundo de Participação dos Estados. Proporcionalidade da MP nº 954/2020. Ausência de periculum in mora. Presença de perigo de demora inverso, em face da urgência na formulação de políticas públicas eficazes no combate à pandemia. Manifestação pelo indeferimento do pedido cautelar." Na mesma data, foram apresentadas informações pelo Instituto Brasileiro de Geografia e Estatística – IBGE e pela Agência Nacional de Telecomunicações - ANATEL.

13. Relatado o essencial, decido.

14. Entendo que as condições em que se dá a manipulação de dados pessoais digitalizados, por agentes públicos ou privados, consiste em um dos maiores desafios contemporâneos do direito à privacidade. A Constituição da República confere especial proteção à intimidade, à vida privada, à honra e à imagem das pessoas ao qualificá-las como invioláveis, enquanto direitos fundamentais da personalidade, assegurando indenização pelo dano material ou moral decorrente de sua violação (art. 5º, X). O assim chamado direito à privacidade (right to privacy) e os seus consectários direitos à intimidade, à honra e à imagem emanam do reconhecimento de que a personalidade individual merece ser protegida em todas as suas manifestações. A fim de instrumentalizar tais direitos, a Constituição prevê, no art. 5º, XII, a inviolabilidade do "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 penal".

15. O art. 2º da MP n. 954/2020 impõe às empresas prestadoras do Serviço Telefônico Fixo Comutado – STFC e do Serviço Móvel Pessoal – SMP o compartilhamento, com a Fundação Instituto Brasileiro de Geografia e Estatística – IBGE, da relação de nomes,

números de telefone e endereços de seus consumidores, pessoas físicas ou jurídicas. Tais informações, relacionadas à identificação – efetiva ou potencial – de pessoa natural, configuram dados pessoais e integram, nessa medida, o âmbito de proteção das cláusulas constitucionais assecuratórias da liberdade individual (art. 5º, caput), da privacidade e do livre desenvolvimento da personalidade (art. 5º, X e XII). Sua manipulação e tratamento, desse modo, hão de observar, sob pena de lesão a esses direitos, os limites delineados pela proteção constitucional. Decorrências dos direitos da personalidade, o respeito à privacidade e à autodeterminação informativa foram positivados, no art. 2º, I e II, da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais), como fundamentos específicos da disciplina da proteção de dados pessoais . No clássico artigo The Right to Privacy, escrito a quatro mãos pelos juízes da Suprema Corte dos Estados Unidos Samuel D. Warren e Louis D. Brandeis, já se reconhecia que as mudanças políticas, sociais e econômicas demandam incessantemente o reconhecimento de novos direitos, razão pela qual necessário, de tempos em tempos, redefinir a exata natureza e extensão da proteção à privacidade do indivíduo. Independentemente do seu conteúdo, mutável com a evolução tecnológica e social, no entanto, permanece como denominador comum da privacidade e da autodeterminação o entendimento de que a privacidade somente pode ceder diante de justificativa consistente e legítima. Em seus dizeres, "a invasão injustificada da privacidade individual deve ser repreendida e, tanto quanto possível, prevenida".

16. Cumpre, pois, equacionar se a MP n. 954/2020 exorbitou dos limites traçados pela Constituição ao dispor sobre a disponibilização dos dados pessoais de todos os consumidores dos serviços STFC e SMP, pelos respectivos operadores, a entidade integrante da Administração indireta.

17. Observo que o único dispositivo da MP n. 954/2020 a dispor sobre a finalidade e o modo de utilização dos dados objeto da norma é o § 1º do seu art. 2º. E esse limita-se a enunciar que os dados em questão serão utilizados exclusivamente pela Fundação IBGE para a produção estatística oficial, com o objetivo de realizar entrevistas em caráter não presencial no âmbito de pesquisas domiciliares. Não delimita o objeto da estatística a ser produzida, nem a finalidade específica, tampouco a amplitude. Igualmente não



esclarece a necessidade de disponibilização dos dados nem como serão efetivamente utilizados. Já o art. 1º, parágrafo único, da MP n. 954/2020 apenas dispõe que o ato normativo terá aplicação durante a situação de emergência de saúde pública de importância internacional decorrente da COVID-19. Ainda que se possa associar, por inferência, que a estatística a ser produzida tenha relação com a pandemia invocada como justificativa da edição da MP, tal ilação não se extrai de seu texto. Nessa ordem de ideias, não emerge da Medida Provisória n. 954/2020, nos moldes em que posta, interesse público legítimo no compartilhamento dos dados pessoais dos usuários dos serviços de telefonia, considerados a necessidade, a adequação e a proporcionalidade da medida. E tal dever competia ao Poder Executivo ao editá-la. Nessa linha, ao não definir apropriadamente como e para que serão utilizados os dados coletados, a MP n. 954/2020 não oferece condições para avaliação da sua adequação e necessidade, assim entendidas como a compatibilidade do tratamento com as finalidades informadas e sua limitação ao mínimo necessário para alcançar suas finalidades. Desatende, assim, a garantia do devido processo legal (art. 5º, LIV, da Lei Maior), em sua dimensão substantiva.

18. De outra parte, o art. 3º, I e II, da MP n. 954/2020 dispõe que os dados compartilhados "terão caráter sigiloso" e "serão utilizados exclusivamente para a finalidade prevista no § 1º do art. 2º", e o art. 3º, § 1º, veda ao IBGE compartilhar os dados disponibilizados com outros entes, públicos ou privados. Nada obstante, a MP n. 954/2020 não apresenta mecanismo técnico ou administrativo apto a proteger os dados pessoais de acessos não autorizados, vazamentos acidentais ou utilização indevida, seja na sua transmissão, seja no seu tratamento. Limita-se a delegar a ato do Presidente da Fundação IBGE o procedimento para compartilhamento dos dados, sem oferecer proteção suficiente aos relevantes direitos fundamentais em jogo. Enfatizo: ao não prever exigência alguma quanto a mecanismos e procedimentos para assegurar o sigilo, a higidez e, quando o caso, o anonimato dos dados compartilhados, a MP n. 954/2020 não satisfaz as exigências que exsurgem do texto constitucional no tocante à efetiva proteção de direitos fundamentais dos brasileiros. Essas considerações são corroboradas pela manifestação trazida aos autos pela Agência Nacional de Telecomunicações – ANATEL, que destacou necessária "a observância de extrema cautela no tratamento dos dados de usuários de serviços de

telecomunicações". E recomendou a adoção de medidas visando a adequar a medida à garantia dos princípios estabelecidos na Constituição Federal, na Lei Geral das Telecomunicações e na Lei Geral de Proteção de Dados, de modo a assegurar a proteção da privacidade, da intimidade e dos dados pessoais de usuários de serviços de telecomunicações, mediante: "a) a sólida instrumentalização da relação jurídica que será estabelecida entre o IBGE e cada uma das prestadoras de serviços de telecomunicações demandadas; b) a delimitação específica da finalidade do uso dos dados solicitados; c) a limitação das solicitações ao universo de dados estritamente necessários para o atingimento da finalidade; d) a delimitação do período de uso e da forma de descarte dos dados; e e) a aplicação de boas práticas de segurança, de transparência e de controle."

19. Não bastasse, a ausência de garantias de tratamento adequado e seguro dos dados compartilhados parece-me agravada pela circunstância de que, embora aprovada, ainda não está em vigor a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), definidora dos critérios para a responsabilização dos agentes por eventuais danos ocorridos em virtude do tratamento de dados pessoais.

20. Verifico, ainda, que na mesma data da publicação da MP n. 954/2020 foi editada a Instrução Normativa n. 2, de 17 de abril de 2020, que estabelece procedimentos para disponibilização de dados de empresas de telecomunicações prestadoras de serviço telefônico fixo ou móvel ao Instituto Brasileiro Geográfico e Estatística -IBGE, para fins de suporte à produção de estatística oficial, durante a situação de emergência de saúde pública de importância internacional decorrente do coronavírus. A referida Instrução Normativa teria embasado o envio, em 22.4.2020, segundo noticiado nos autos, de ofícios da Fundação IBGE às empresas de telefonia fixa comutada ou móvel pessoal, solicitando, com urgência, o compartilhamento imediato de dados, não obstante o prazo de sete fixados pela Medida Provisória 954/2020 e a determinação deste Supremo Tribunal Federal para a prestação de informações acerca do conteúdo deste ato normativo (doc. 24 do processo eletrônico).

21. Saliento, também, que a análise da tramitação do projeto de lei de conversão da Medida Provisória 954/2020 revela terem sido apresentadas, até o momento, 344 propostas



de emenda. Em significativo número, propugnada a restrição da norma aos dados estritamente necessários, bem como a necessidade de elaboração de relatório de impacto de segurança da informação anterior à coleta e uso dos dados (e não posterior, como veiculado), além da maior transparência na definição da finalidade e do uso dos dados compartilhados.

22. Presente, à luz do exposto, o fumus boni juris, tenho por satisfeito igualmente o periculum in mora, uma vez que a determinação do imediato compartilhamento de dados leva à eficácia plena do ato normativo questionado. Não se subestima a gravidade do cenário de urgência decorrente da crise sanitária nem a necessidade de formulação de políticas públicas que demandam dados específicos para o desenho dos diversos quadros de enfrentamento. O seu combate, todavia, não pode legitimar o atropelo de garantias fundamentais consagradas na Constituição.

23. Reforço, em cumprimento ao dever de justificação decisória, no âmbito de medida liminar, que a adequada tutela do direito à intimidade, privacidade e proteção de dados pessoais é estruturada pela característica da inviolabilidade. Vale dizer, uma vez afrontada a norma de proteção de tais direitos, o ressarcimento se apresenta como tutela insuficiente aos deveres de proteção.

24. Nesse contexto, e a fim de prevenir danos irreparáveis à intimidade e ao sigilo da vida privada de mais de uma centena de milhão de usuários dos serviços de telefonia fixa e móvel, com o caráter precário próprio aos juízos perfunctórios e sem prejuízo de exame mais aprofundado quando do julgamento do mérito, defiro a medida cautelar requerida, ad referendum do Plenário desta Suprema Corte, para suspender a eficácia da Medida Provisória n. 954/2020, determinando, em consequência, que o Instituto Brasileiro de Geografia e Estatística – IBGE se abstenha de requerer a disponibilização dos dados objeto da referida medida provisória e, caso já o tenha feito, que suste tal pedido, com imediata comunicação à(s) operadora(s) de telefonia.

25. Por fim, considerando que as ações diretas de inconstitucionalidade nºs 6388, 6389, 6390 e 6393, a mim distribuídas por prevenção (art. 77-B, RISTF), igualmente impugnam a validade constitucional da Medida Provisória n. 954/2020, determino a tramitação

conjunta dos feitos, com a reprodução desta decisão nos autos respectivos. À Secretaria Judiciária. Publique-se. Intime-se, com urgência. Brasília, 24 de abril de 2020. Ministra Rosa Weber Relatora.

Link: **https://jurisprudencia.stf.jus.br/pages/search/despacho1095308/false**

## Comentários

As decisões do STF indicam que a manipulação de dados pessoais digitalizados, por agentes públicos ou privados, tem sido um dos maiores desafios contemporâneos do direito à privacidade. Tal dificuldade pode ser atribuída a velocidade e mutabilidade das ferramentas tecnológicas em descompasso com as legislações vigentes.

Observa-se que o STF compreende o registro de dados pessoais em sentido mais amplo, abrangendo tudo que diga respeito ao interessado, seja de modo direto ou indireto que possa causar dano ao direito de privacidade, de acordo com o que agora está regulado pelo art. 5.º da LGPD.

Nota-se também diferença no tratamento da proteção de dados envolvendo o Poder Público e as entidades privadas. No caso do Poder Público, a partir da aplicação da norma do art. 5º, XII da CF, tanto pode ocorrer a possibilidade de compartilhamento de dados como a restrição no tratamento de dados. Em relação as entidades privadas o cuidado reside na proteção do sigilo de dados pessoais.

De um modo geral, as decisões evidenciam que o STF, mesmo antes da entrada em vigor da LGPD, já havia assimilado os fundamentos doutrinários da proteção jurídica de dados pessoais, a partir do paradigma de autodeterminação informativa. O caminho percorrido pela Corte na proteção de dados pessoais encontra o ponto de consolidação que pode ser fixado na solução normativa dada pela Ministra Rosa Weber na **ADI 6387 MC / DF - DISTRITO FEDERAL,** em que se observa na fundamentação da decisão a invocação de elementos constantes das normas da LGPD que, naquela ocasião, ainda não havia entrado em vigor. Assim, a aplicação da LGPD encontrará consolidada uma cultura jurisprudencial no STF de proteção de dados pessoais.



# STJ

## Competência

De acordo com o art 105 da Constituição Federal compete ao Superior Tribunal de Justiça (STJ), atuar como Corte de uniformização da interpretação das leis federais em todo o país.

## Decisões

**REsp 1758799 / MG**

RECURSO ESPECIAL. FUNDAMENTO NÃO IMPUGNADO. SÚM. 283/STF. AÇÃO DE COMPENSAÇÃO DE DANO MORAL. BANCO DE DADOS. COMPARTILHAMENTO DE INFORMAÇÕES PESSOAIS. DEVER DE INFORMAÇÃO. VIOLAÇÃO. DANO MORAL IN RE IPSA. JULGAMENTO: CPC/15.

1. Ação de compensação de dano moral ajuizada em 10/05/2013, da qual foi extraído o presente recurso especial, interposto em 29/04/2016 e atribuído ao gabinete em 31/01/2017.

2. O propósito recursal é dizer sobre: (i) a ocorrência de inovação recursal nas razões da apelação interposta pelo recorrido; (ii) a caracterização do dano moral em decorrência da disponibilização/comercialização de dados pessoais do recorrido em banco de dados mantido pela recorrente.

3. A existência de fundamento não impugnado - quando suficiente para a manutenção das conclusões do acórdão recorrido - impede a apreciação do recurso especial (súm. 283/STF).

4. A hipótese dos autos é distinta daquela tratada no julgamento do REsp 1.419.697/RS (julgado em 12/11/2014, pela sistemática dos recursos repetitivos, DJe de 17/11/2014), em que a Segunda Seção decidiu que, no sistema credit scoring, não se pode exigir o prévio e expresso consentimento do consumidor avaliado, pois não constitui um cadastro ou banco de dados, mas um modelo estatístico.

5. A gestão do banco de dados impõe a estrita observância das exigências contidas nas respectivas normas de regência - CDC e Lei 12.414/2011 - dentre as quais se destaca o

dever de informação, que tem como uma de suas vertentes o dever de comunicar por escrito ao consumidor a abertura de cadastro, ficha, registro e dados pessoais e de consumo, quando não solicitada por ele.

6. O consumidor tem o direito de tomar conhecimento de que informações a seu respeito estão sendo arquivadas/comercializadas por terceiro, sem a sua autorização, porque desse direito decorrem outros dois que lhe são assegurados pelo ordenamento jurídico: o direito de acesso aos dados armazenados e o direito à retificação das informações incorretas.

7. A inobservância dos deveres associados ao tratamento (que inclui a coleta, o armazenamento e a transferência a terceiros) dos dados do consumidor - dentre os quais se inclui o dever de informar - faz nascer para este a pretensão de indenização pelos danos causados e a de fazer cessar, imediatamente, a ofensa aos direitos da personalidade.

8. Em se tratando de compartilhamento das informações do consumidor pelos bancos de dados, prática essa autorizada pela Lei 12.414/2011 em seus arts. 4º, III, e 9º, deve ser observado o disposto no art. 5º, V, da Lei 12.414/2011, o qual prevê o direito do cadastrado ser informado previamente sobre a identidade do gestor e sobre o armazenamento e o objetivo do tratamento dos dados pessoais

9. O fato, por si só, de se tratarem de dados usualmente fornecidos pelos próprios consumidores quando da realização de qualquer compra no comércio, não afasta a responsabilidade do gestor do banco de dados, na medida em que, quando o consumidor o faz não está, implícita e automaticamente, autorizando o comerciante a divulgá-los no mercado; está apenas cumprindo as condições necessárias à concretização do respectivo negócio jurídico entabulado apenas entre as duas partes, confiando ao fornecedor a proteção de suas informações pessoais.

10. Do mesmo modo, o fato de alguém publicar em rede social uma informação de caráter pessoal não implica o consentimento, aos usuários que acessam o conteúdo, de utilização de seus dados para qualquer outra finalidade, ainda mais com fins lucrativos.

11. Hipótese em que se configura o dano moral in re ipsa.



12. Em virtude do exame do mérito, por meio do qual foram rejeitadas as teses sustentada pela recorrente, fica prejudicada a análise da divergência jurisprudencial.

13. Recurso especial conhecido em parte e, nessa extensão, desprovido.

(REsp 1758799/MG, Rel. Ministra NANCY ANDRIGHI, TERCEIRA TURMA, julgado em 12/11/2019, DJe 19/11/2019)

Link: **https://scon.stj.jus.br/SCON/jurisprudencia/toc.jsp?livre=201700065219.REG.**

**REsp 1660168 / RJ**

RECURSO ESPECIAL. DIREITO CIVIL. AÇÃO DE OBRIGAÇÃO DE FAZER. 1. OMISSÃO, CONTRADIÇÃO OU OBSCURIDADE. AUSÊNCIA. 2. JULGAMENTO EXTRA PETITA. NÃO CONFIGURADO. 3. PROVEDOR DE APLICAÇÃO DE PESQUISA NA INTERNET. PROTEÇÃO A DADOS PESSOAIS. POSSIBILIDADE JURÍDICA DO PEDIDO. DESVINCULAÇÃO ENTRE NOME E RESULTADO DE PESQUISA. PECULIARIDADES FÁTICAS. CONCILIAÇÃO ENTRE O DIREITO INDIVIDUAL E O DIREITO COLETIVO À INFORMAÇÃO. 4. MULTA DIÁRIA APLICADA. VALOR INICIAL EXORBITANTE. REVISÃO EXCEPCIONAL. 5. RECURSO ESPECIAL PARCIALMENTE PROVIDO.

1. Debate-se a possibilidade de se determinar o rompimento do vínculo estabelecido por provedores de aplicação de busca na internet entre o nome do prejudicado, utilizado como critério exclusivo de busca, e a notícia apontada nos resultados.

2. O Tribunal de origem enfrentou todas as questões postas pelas partes, decidindo nos estritos limites da demanda e declinando, de forma expressa e coerente, todos os fundamentos que formaram o livre convencimento do Juízo.

3. A jurisprudência desta Corte Superior tem entendimento reiterado no sentido de afastar a responsabilidade de buscadores da internet pelos resultados de busca apresentados, reconhecendo a impossibilidade de lhe atribuir a função de censor e impondo ao prejudicado o direcionamento de sua pretensão contra os provedores de conteúdo, responsáveis pela disponibilização do conteúdo indevido na internet. Precedentes.

4. Há, todavia, circunstâncias excepcionalíssimas em que é necessária a intervenção pontual do Poder Judiciário para fazer cessar o vínculo criado, nos bancos de dados dos

provedores de busca, entre dados pessoais e resultados da busca, que não guardam relevância para interesse público à informação, seja pelo conteúdo eminentemente privado, seja pelo decurso do tempo.

5. Nessas situações excepcionais, o direito à intimidade e ao esquecimento, bem como a proteção aos dados pessoais deverá preponderar, a fim de permitir que as pessoas envolvidas sigam suas vidas com razoável anonimato, não sendo o fato desabonador corriqueiramente rememorado e perenizado por sistemas automatizados de busca.

6. O rompimento do referido vínculo sem a exclusão da notícia compatibiliza também os interesses individual do titular dos dados pessoais e coletivo de acesso à informação, na medida em que viabiliza a localização das notícias àqueles que direcionem sua pesquisa fornecendo argumentos de pesquisa relacionados ao fato noticiado, mas não àqueles que buscam exclusivamente pelos dados pessoais do indivíduo protegido.

7. No caso concreto, passado mais de uma década desde o fato noticiado, ao se informar como critério de busca exclusivo o nome da parte recorrente, o primeiro resultado apresentado permanecia apontando link de notícia de seu possível envolvimento em fato desabonador, não comprovado, a despeito da existência de outras tantas informações posteriores a seu respeito disponíveis na rede mundial.

8. O arbitramento de multa diária deve ser revisto sempre que seu valor inicial configure manifesta desproporção, por ser irrisório ou excessivo, como é o caso dos autos.

9. Recursos especiais parcialmente providos.

(REsp 1660168/RJ, Rel. Ministra NANCY ANDRIGHI, Rel. p/ Acórdão Ministro MARCO AURÉLIO BELLIZZE, TERCEIRA TURMA, julgado em 08/05/2018, DJe 05/06/2018)

Link: **https://scon.stj.jus.br/SCON/jurisprudencia/toc.jsp?livre=201402917771.REG.**

**REsp 1348532 / SP**

RECURSO ESPECIAL. CONSUMIDOR. CERCEAMENTO DE DEFESA. NÃO OCORRÊNCIA. CONTRATO DE CARTÃO DE CRÉDITO. CLÁUSULAS ABUSIVAS. COMPARTILHAMENTO DE DADOS PESSOAIS. NECESSIDADE DE OPÇÃO POR SUA NEGATIVA. DESRESPEITO AOS PRINCÍPIOS DA TRANSPARÊNCIA E CONFIANÇA. ABRANGÊNCIA DA SENTENÇA. ASTREINTES. RAZOABILIDADE.

1. É facultado ao Juízo proferir sua decisão, desde que não haja necessidade de produzir provas em audiência, assim como, nos termos do que preceitua o princípio da livre persuasão racional, avaliar as provas requeridas e rejeitar aquelas que protelariam o andamento do processo, em desrespeito ao princípio da celeridade.

2. A Anadec - Associação Nacional de Defesa do Consumidor, da Vida e dos Direitos Civis tem legitimidade para, em ação civil pública, pleitear o reconhecimento de abusividade de cláusulas insertas em contrato de cartão de crédito. Precedentes.

3. É abusiva e ilegal cláusula prevista em contrato de prestação de serviços de cartão de crédito, que autoriza o banco contratante a compartilhar dados dos consumidores com outras entidades financeiras, assim como com entidades mantenedoras de cadastros positivos e negativos de consumidores, sem que seja dada opção de discordar daquele compartilhamento.

4. A cláusula posta em contrato de serviço de cartão de crédito que impõe a anuência com o compartilhamento de dados pessoais do consumidor é abusiva por deixar de atender a dois princípios importantes da relação de consumo: transparência e confiança.

5. A impossibilidade de contratação do serviço de cartão de crédito, sem a opção de negar o compartilhamento dos dados do consumidor, revela exposição que o torna indiscutivelmente vulnerável, de maneira impossível de ser mensurada e projetada.

6. De fato, a partir da exposição de seus dados financeiros abre-se possibilidade para intromissões diversas na vida do consumidor. Conhecem-se seus hábitos, monitoram-se a maneira de viver e a forma de efetuar despesas. Por isso, a imprescindibilidade da autorização real e espontânea quanto à exposição.

7. Considera-se abusiva a cláusula em destaque também porque a obrigação que ela anuncia se mostra prescindível à execução do serviço contratado, qual seja obtenção de crédito por meio de cartão.

8. Não se estende a abusividade, por óbvio, à inscrição do nome e CPF de eventuais devedores em cadastros negativos de consumidores (SPC, SERASA, dentre outros), por inadimplência, uma vez que dita providência encontra amparo em lei (Lei n. 8.078/1990, arts. 43 e 44).

9. A orientação fixada pela jurisprudência da Corte Especial do STJ, em recurso repetitivo, no que se refere à abrangência da sentença prolatada em ação civil pública, é que "os efeitos e a eficácia da sentença não estão circunscritos a lindes geográficos, mas aos limites objetivos e subjetivos do que foi decidido, levando-se em conta, para tanto, sempre a extensão do dano e a qualidade dos interesses metaindividuais postos em juízo (arts. 468, 472 e 474, CPC e 93 e 103, CDC)" (REsp 1.243.887/PR, Rel. Ministro LUIS FELIPE SALOMÃO, CORTE ESPECIAL, DJe de 12/12/2011).

10. É pacífico o entendimento no sentido de que a revisão da multa fixada, para o caso de descumprimento de ordem judicial, só será possível, nesta instância excepcional, quando se mostrar irrisória ou exorbitante, o que, a meu ver, se verifica na hipótese, haja vista tratar-se de multa diária no valor de R$10.000,00 (dez mil reais).

11. Recurso especial parcialmente provido.

(REsp 1348532/SP, Rel. Ministro LUIS FELIPE SALOMÃO, QUARTA TURMA, julgado em 10/10/2017, DJe 30/11/2017)

Link: **https://scon.stj.jus.br/SCON/jurisprudencia/toc.jsp?livre=201202108054.REG.**

**EDcl no REsp 1630889 / DF**

EMBARGOS DE DECLARAÇÃO. RECURSO ESPECIAL. DIREITO DO CONSUMIDOR. BANCOS DE DADOS. PROTEÇÃO AO CRÉDITO. PRIVACIDADE E INTIMIDADE. AUTODETERMINAÇÃO INFORMATIVA. DIREITOS FUNDAMENTAIS. EFICÁCIA HORIZONTAL. PRINCÍPIO DA MÁXIMA EFETIVIDADE. OBRIGAÇÃO DE NÃO FAZER. ANOTAÇÕES. CARTÓRIOS DE PROTESTO. TERMO INICIAL DO PRAZO. ART. 43, § 1º, DO CDC. DATA DO VENCIMENTO DA DÍVIDA. MODULAÇÃO DOS EFEITOS. ART. 927, § 3º, DO CPC/15. PRINCÍPIO. PROTEÇÃO DA CONFIANÇA LEGÍTIMA. REGIME DE TRANSIÇÃO. ART. 23 DA LINDB. ÔNUS E PREJUÍZOS ANORMAIS OU EXCESSIVOS.



1 O propósito dos presentes embargos de declaração é determinar se são necessárias a modulação dos efeitos da condenação contida no acórdão embargado e a adoção de regime de transição para que a embargante se adeque ao comando contido em seu dispositivo (arts. 927, § 3º, do CPC/15 e 23 da LINDB).

2. A modulação de efeitos de decisão que supera orientação jurisprudencial é matéria apreciável de ofício, razão pela qual não configura inovação recursal.

3. O dever dos Tribunais de manter sua jurisprudência estável, íntegra e coerente cumpre o propósito de garantir a isonomia de ordem material e a proteção da confiança e da expectativa legítima do jurisdicionado, fornecendo-lhe um modelo seguro de conduta de modo a tornar previsíveis as consequências de seus atos.

4. A força vinculante do precedente, em sentido estrito, bem como da jurisprudência, em sentido substancial, decorre de sua capacidade de servir de diretriz para o julgamento posterior em casos análogos e de, assim, criar nos jurisdicionados a legítima expectativa de que serão seguidos pelo próprio órgão julgador e órgãos hierarquicamente inferiores e, como consequência, sugerir para o cidadão um padrão de conduta a ser seguido com estabilidade.

5. A modulação de efeitos do art. 927, § 3º, do CPC/15 deve ser utilizada com parcimônia, de forma excepcional e em hipóteses específicas, em que o entendimento superado tiver sido efetivamente capaz de gerar uma expectativa legítima de atuação nos jurisdicionados e, ainda, o exigir o interesse social envolvido.

6. O regime de transição do art. 23 da LINDB está em íntima conexão com o princípio da menor onerosidade da regularização, previsto no art. 21, parágrafo único, de referido diploma legal, segundo o qual não se pode impor aos sujeitos atingidos pela modificação de jurisprudência ônus ou perdas anormais ou excessivos.

7. Os direitos à intimidade e à proteção da vida privada, diretamente relacionados à utilização de dados pessoais por bancos de dados de proteção ao crédito, consagram o direito à autodeterminação informativa e encontram guarida constitucional no art. 5º, X, da Carta Magna, que deve ser aplicado nas relações entre particulares por força de

sua eficácia horizontal e privilegiado por imposição do princípio da máxima efetividade dos direitos fundamentais.

8. In casu, ao menos desde o julgamento pela 3ª Turma do REsp 1316117/SC, ocorrido em 26/04/2016, não há jurisprudência consolidada em relação ao termo inicial do prazo máximo de inscrição da anotação nos cadastros de proteção ao crédito, o que permite concluir pela inexistência de jurisprudência em sentido substancial, capaz de ensejar nos jurisdicionados uma confiança racionalmente aceitável de estabilidade capaz de subsidiar uma legítima expectativa de certeza objetiva de resposta jurisdicional.

9. Ademais, não existe desproporcionalidade na imediata adoção da vedação ao registro de anotações negativas sem que conste a data de vencimento da dívida, pois a mera suspensão, até efetiva regularização do procedimento, da anotação de registros provenientes de cartórios de protesto que não contenham essa informação, não gera ônus excessivos ou desproporcionais para a embargante e evita a perpetuação dessa lesão aos direitos dos consumidores.

10. Embargos de declaração acolhidos sem efeitos infringentes.

(EDcl no REsp 1630889/DF, Rel. Ministra NANCY ANDRIGHI, TERCEIRA TURMA, julgado em 27/11/2018, DJe 06/12/2018)

Link: **https://scon.stj.jus.br/SCON/jurisprudencia/toc.jsp?livre=201602636651.REG.**

**REsp 1582981 / RJ**

CIVIL E CONSUMIDOR. RECURSO ESPECIAL. 1. INTERNET. PROVEDOR DE PESQUISA. EXIBIÇÃO DE RESULTADOS. POTENCIAL OFENSIVO. AUSÊNCIA. DANO MORAL. AFASTADO. 2. RELAÇÃO DE CONSUMO. INCIDÊNCIA DO CDC. GRATUIDADE DO SERVIÇO. INDIFERENÇA. CORRESPONDÊNCIA ENTRE OS RESULTADOS E A PESQUISA. AUSÊNCIA. EXPECTATIVA RAZOÁVEL. FALHA DO SERVIÇO. CONFIGURAÇÃO. 3. OBRIGAÇÃO DE FAZER PERSONALÍSSIMA. DECISÃO JUDICIAL. INÉRCIA RENITENTE. MULTA COMINATÓRIA. FIXAÇÃO DE PATAMAR ESTÁTICO. INSUFICIÊNCIA RECONHECIDA. 4. RECURSOS ESPECIAIS PARCIALMENTE PROVIDOS.



1. Recurso especial em que se debate a responsabilidade civil decorrente da discrepância entre o resultado de busca e a alteração do conteúdo danoso inserido em sítio eletrônico, bem como a obrigatoriedade de atualização dos resultados de busca conforme o novo conteúdo disponível no momento da consulta.

2. Nos termos da jurisprudência desta Corte Superior, os provedores de pesquisa fornecem ferramentas para localização, dentro do universo virtual, de acesso público e irrestrito, de conteúdos relacionados aos termos informados para pesquisa.

3. Não contém aptidão para causar dano moral a exibição dos resultados na forma de índice, em que se relacionam links para páginas em que há conteúdos relacionados aos termos de busca, independente do potencial danoso do conteúdo em si ou dos termos da busca inseridos pelos internautas.

4. Os provedores de pesquisa podem ser excepcionalmente obrigados a eliminar de seu banco de dados resultados incorretos ou inadequados, especialmente quando inexistente relação de pertinência entre o conteúdo do resultado e o critério pesquisado.

5. A ausência de congruência entre o resultado atual e os termos pesquisados, ainda que decorrentes da posterior alteração do conteúdo original publicado pela página, configuram falha na prestação do serviço de busca, que deve ser corrigida nos termos do art. 20 do CDC, por frustrarem as legítimas expectativas dos consumidores.

6. A multa cominatória tem por finalidade essencial o desincentivo à recalcitrância contumaz no cumprimento de decisões judiciais, de modo que seu valor deve ser dotado de força coercitiva real.

7. A limitação da multa cominatória em patamar estático pode resultar em elemento determinante no cálculo de custo-benefício, no sentido de configurar o desinteresse no cumprimento das decisões, engessando a atividade jurisdicional e tolhendo a eficácia das decisões.

8. A multa diária mostrou-se insuficiente, em face da concreta renitência quanto ao cumprimento voluntário da decisão judicial, impondo sua majoração excepcional por esta Corte Superior, com efeitos ex nunc, em observância ao princípio da não surpresa, dever lateral à boa-fé objetiva processual expressamente consagrado no novo CPC (art. 5º).

9. Recursos especiais parcialmente providos.

(REsp 1582981/RJ, Rel. Ministro MARCO AURÉLIO BELLIZZE, TERCEIRA TURMA, julgado em 10/05/2016, DJe 19/05/2016)

Link: https://scon.stj.jus.br/SCON/jurisprudencia/toc.jsp?livre=201502238660.REG.

**REsp 1068904 / RS**

RECURSO ESPECIAL - AÇÃO CAUTELAR DE EXIBIÇÃO DE DOCUMENTOS - INFORMAÇÕES ACERCA DA ORIGEM DE MENSAGENS ELETRÔNICAS DIFAMATÓRIAS ANÔNIMAS PROFERIDAS POR MEIO DA INTERNET - LIDE CONTEMPORÂNEA - POSSIBILIDADE DE IDENTIFICAÇÃO DO AUTOR - ACESSO AOS DADOS CADASTRAIS DO TITULAR DE CONTA DE E-MAIL - MANDADO JUDICIAL - NECESSIDADE - SIGILO DE DADOS - PRESERVAÇÃO - ÔNUS SUCUMBENCIAIS - CONDENAÇÃO - IMPOSSIBILIDADE - AUSÊNCIA DE RESISTÊNCIA DO PROVEDOR - PRINCÍPIO DA CAUSALIDADE - AFASTAMENTO - NECESSIDADE - RECURSO ESPECIAL PROVIDO.

I - A presente controvérsia é uma daquelas questões que a vida moderna nos impõe analisar. Um remetente anônimo utiliza-se da Internet, para e por meio dela, ofender e denegrir a imagem e reputação de outrem. Outrora, a carta era um dos meios para tal. Doravante, o e-mail e as mensagens eletrônicas (SMS), a substituíram. Todavia, o fim continua o mesmo: ofender sem ser descoberto. O caráter anônimo de tais instrumentos pode até incentivar tal conduta ilícita. Todavia, os meios existentes atualmente permitem rastrear e, portanto, localizar o autor das ofensas, ainda que no ambiente eletrônico.

II - À luz do que dispõe o art. 5º, inciso XII, da Constituição Federal, infere-se que, somente por ordem judicial, frise-se, a ora recorrente, UNIVERSO ONLINE S. A., poderia permitir acesso a terceiros ao seu banco de dados cadastrais.

III - A medida cautelar de exibição de documentos é ação e, portanto, nessa qualidade, é devida a condenação da parte-ré ao pagamento dos honorários advocatícios, por força do princípio da causalidade.



IV - Na espécie, contudo, não houve qualquer resistência da ora recorrente que, inclusive, na própria contestação, admitiu a possibilidade de fornecer os dados cadastrais, desde que, mediante determinação judicial, sendo certo que não poderia ser compelida, extrajudicialmente, a prestar as informações à autora, diante do sigilo constitucionalmente assegurado.

V - Dessa forma, como o acesso a dados cadastrais do titular de conta de e-mail (correio eletrônico) do provedor de Internet só pode ser determinada pela via judicial, por meio de mandado, não há que se falar em aplicação do princípio da causalidade, apto a justificar a condenação nos ônus sucumbenciais.

VI - Recurso especial provido.

(REsp 1068904/RS, Rel. Ministro MASSAMI UYEDA, TERCEIRA TURMA, julgado em 07/12/2010, DJe 30/03/2011)

Link: https://scon.stj.jus.br/SCON/jurisprudencia/toc.jsp?livre=200801381961.REG.

**REsp 1274971 / RS**

DIREITO CIVIL. AÇÃO CAUTELAR. AGRAVO DE INSTRUMENTO. PROVEDOR DE BLOGs. MENSAGEM DE CONTEÚDO OFENSIVO. INFORMAÇÃO DO URL PELO OFENDIDO.

1. O provedor de hospedagem de blogs não está obrigado a realizar a prévia fiscalização das informações que neles circulam. Assim, não necessita de obter dados relativos aos conteúdos veiculados, mas apenas referentes aos autores dos blogs.

2. Se em algum blog for postada mensagem ofensiva à honra de alguém, o interessado na responsabilização do autor deverá indicar o URL das páginas em que se encontram os conteúdos consideradas ofensivos. Não compete ao provedor de hospedagem de blogs localizar o conteúdo dito ofensivo por se tratar de questão subjetiva, cabendo ao ofendido individualizar o que lhe interessa e fornecer o URL. Caso contrário, o provedor não poderá garantir a fidelidade dos dados requeridos pelo ofendido.

3. Recurso especial conhecido e provido.

(REsp 1274971/RS, Rel. Ministro JOÃO OTÁVIO DE NORONHA, TERCEIRA TURMA, julgado em 19/03/2015, DJe 26/03/2015)

Link: **https://scon.stj.jus.br/SCON/jurisprudencia/toc.jsp?livre=201102075972.REG.**

### Comentários

As decisões do STJ tutelam dados pessoais, o direito da personalidade e o sigilo, a partir das normas do Código de Defesa do Consumidor (CDC)- Lei nº8.078/90, do Código Civil de 2020 (CC)- Lei nº10.406/02, do Código de Processo Civil – Lei nº13.105/15, e da Lei do Cadastro Positivo; Lei 12.414/2011.

Percebe-se que o Código de Defesa do Consumidor é aplicado na maioria dos julgados que envolvem a gestão de dados, mesmo que o fornecedor não tenha fins lucrativos, estando configurada uma relação de consumo, implícita na prestação de serviços.

A gestão do banco de dados pelos fornecedores configura relação de consumo e implica a observância das exigências constantes do Código de Defesa do Consumidor e da Lei do Cadastro Positivo, em que acentuado o dever de informação, ou seja de comunicar por escrito o consumidor sobre eventuais aberturas de cadastro, ficha, registro, dados pessoais e de consumo, quando não solicitadas pelo titular, sob pena de indenização pelos danos causados em ofensa aos direitos da personalidade protegidos no Código Civil.

As decisões também tratam da questão polêmica a respeito da responsabilidade dos buscadores da internet pelos resultados de busca realizados. O STJ entende tratar-se de questão subjetiva, não atribuindo ao buscador ou provedor de hospedagem a função de censor, cabendo ao prejudicado buscar tutela jurisdicional quando sofrer prejuízos. A parte ofendida deve provocar o Poder Judiciário para fazer cessar os efeitos do que foi informado, quando a informação não guardar relevante interesse público ou em razão do decurso do tempo. Nestas hipóteses prepondera o direito à intimidade e ao esquecimento, bem como a proteção aos dados pessoais que pode impor a retirada de dados da rede.

Como se observa, as decisões do STJ já incorporaram os fundamentos da proteção de dados. A aplicação da LGPD contribuirá para o refinamento na forma de proteção ao direito a informação a exemplo do que consta do art. 9.º da referida lei.



Assim, em termos de competência do STJ, a entrada em vigor da LGPD servirá para complementar a sistematização das decisões acerca da proteção de dados que envolva relações privadas (civis e de consumo).

## Tribunal Regional Federal da 4.ª Região – TRF4

### Competência

O Tribunal Regional Federal da 4ª Região (TRF4), tem competência territorial nos Estados do Rio Grande do Sul, Santa Catarina e Paraná. A competência do TRF4 está definida no art. 109 da Constituição Federal e envolve ações em que existente interesse da União Federal, autarquias e empresas públicas, bem como causas envolvendo matéria previdenciária, execuções fiscais e infrações penais praticadas em detrimento dos bens e serviços destas entidades autárquicas ou empresas públicas federais.

### Decisões

**ACR 5000815-62.2017.4.04.7017**

EMENTA: PENAL. RECEPTAÇÃO. ARTIGO 180, CAPUT, DO CÓDIGO PENAL. USO DE DOCUMENTO PÚBLICO FALSO. ARTIGOS 304 E 297 DO CÓDIGO PENAL. INÉPCIA DA DENÚNCIA. INOCORRÊNCIA. VISUALIZAÇÃO, PELA POLÍCIA, DE MENSAGEM NO CELULAR DOS FLAGRADOS SEM AUTORIZAÇÃO JUDICIAL. NULIDADE. INOCORRÊNCIA. MATERIALIDADE, AUTORIA E DOLO COMPROVADOS. DESCLASSIFICAÇÃO PARA RECEPTAÇÃO CULPOSA. NÃO CABIMENTO.

1. Não é inepta a denúncia que esclarece o fato criminoso que se imputa ao acusado "com todas as suas circunstâncias", ou seja, delimitando todos os elementos indispensáveis à sua perfeita individualização.

2. O direito à intimidade comporta relativização, não sendo absoluto. No momento em que está ocorrendo um crime a proteção deve ser à sociedade, e não ao particular.

3. Comprovada a materialidade, a autoria e o dolo dos delitos de receptação e de uso de documento falso narrados na denúncia, pela condução de veículo que se sabia ser

produto de crime, e pela apresentação, a Policiais Rodoviários Federais, de Certificado de Registro e Licenciamento de Veículo (CRLV) inautêntico.

4. Os dados fáticos que envolveram os delitos possibilitam um juízo seguro acerca do dolo na conduta do acusado, pois demonstram que ele conhecia a origem do veículo adquirido e a falsidade do documento.

5. Apelação criminal improvida. (TRF4, ACR 5000815-62.2017.4.04.7017, OITAVA TURMA, Relator JOÃO PEDRO GEBRAN NETO, juntado aos autos em 05/03/2020).

Link: https://jurisprudencia.trf4.jus.br/pesquisa/citacao.php?doc=TRF421011930

**AC 5036793-16.2015.4.04.7100**

Apelação cível. ação civil pública. consumidor. dever de informação. inexistência de violação ao artigo 5º, incisos X e XII, da Constituição. interesse processual. cumprimento provisório do julgado. possibilidade. Artigo 25 da Resolução anatel nº 426/2005 e artigo 91 da resolução anatel nº 477/2007. MULTA diária em caso de descumprimento. indenização. danos morais coletivos.

1. Não há de se falar em ausência de interesse processual em relação ao pedido de fiscalização por parte da ANATEL, sob o argumento de que se trata de obrigação legal da Agência, à medida que o fundamento da pretensão é justamente a suposta ausência da efetiva fiscalização, o que dá azo, naturalmente, ao acesso ao Judiciário.

2. O art. 1.012 do CPC (aplicável subsidiariamente à Ação Civil Pública, conforme o art. 19 da Lei nº 7.347/1985) aponta que a regra é a execução imediata do julgado, sendo a atribuição de efeito suspensivo, a exceção. De uma leitura "contrario sensu", pode-se inferir que, não sendo hipótese elencada no art. 1.012 do CPC, a apelação necessariamente será recebida somente no efeito devolutivo. No caso, não há menção na sentença, no sentido de que as apelações interpostas seriam recebidas com efeito suspensivo. Assim, possível o cumprimento provisório da sentença.

3. A matéria em tela encontra-se regulamentada pela ANATEL, nos termos do art. 25 da Resolução nº 426/2005 e art. 91 da Resolução nº 477/2007.



4. O pleito da inicial é de que a operadora forneça apenas o código de acesso do telefone originador quando solicitado pelo cliente ou pelas autoridades de investigação criminal, sem nenhum outro dado que permita a identificação do usuário. Assim, não há qualquer valor individual relacionado à intimidade ou privacidade que possa ser violado com essa medida.

5. Resta claro que o fornecimento ao consumidor do número originador da chamada telefônica recebida não se confunde com a divulgação de dados cadastrais, tampouco com a divulgação do conteúdo da conversa, os quais estão protegidos por sigilo. Por isso, não há violação aos direitos constitucionais previstos no art. 5º, X e XII, da Constituição.

6. Restou demonstrado nos autos que a Oi S/A descumpre, no mínimo desde 2010, a legislação do setor de telefonia em nosso país, devendo ser acolhida a pretensão do MPF.

7. O objetivo da multa diária não é penalizar a parte que descumpre a ordem, mas garantir a efetividade do comando judicial e, certamente o magistrado singular considerou as circunstâncias do caso concreto para mantê-la em R$ 1.000,00 (um mil reais), valor suficiente a compelir ao cumprimento, podendo, a todo tempo, ser redimensionada.

8. Relativamente à condenação ao pagamento de indenização por danos morais coletivos, constatada a insuficiência do serviço público e da fiscalização da agência reguladora, em prejuízo da coletividade, tal condenação vai ao encontro do posicionamento desta Corte Regional em casos semelhantes. (TRF4, AC 5036793-16.2015.4.04.7100, TERCEIRA TURMA, Relatora MARGA INGE BARTH TESSLER, juntado aos autos em 03/06/2020).

Link: https://jurisprudencia.trf4.jus.br/pesquisa/citacao.php?doc=TRF421684065

**AG 5012386-27.2020.4.04.0000**

EMENTA: AGRAVO DE INSTRUMENTO. EXECUÇÃO FISCAL. ADMINISTRAÇÃO PÚBLICA FEDERAL. ÓRGÃO. RENAJUD. DESNECESSIDADE. Como o Decreto nº 8.789, de 2016, estabelece o compartilhamento de dados entre os órgãos e entidades da administração pública federal, dentre os quais se encontram os dados sobre veículos, desnecessária a intervenção do Poder Judiciário para que realize a consulta ao sistema Renajud, devendo a autarquia exequente trazer aos autos a informação sobre veículo do executado, para

fim de efetivação da restrição por parte do Juízo. (TRF4, AG 5012386-27.2020.4.04.0000, SEGUNDA TURMA, Relator RÔMULO PIZZOLATTI, juntado aos autos em 03/06/2020)

Link:https://jurisprudencia.trf4.jus.br/pesquisa/citacao.php?doc=TRF421667790

**ACR 5018683-62.2012.4.04.7200**

EMENTA: PENAL. CRIME CONTRA A ORDEM TRIBUTÁRIA. ART. 1º, I E II, DA LEI Nº 8.137/90. CERCEAMENTO DE DEFESA. INEXISTÊNCIA. COMPARTILHAMENTO DE DADOS BANCÁRIOS E FISCAIS SEM AUTORIZAÇÃO JUDICIAL. AUSÊNCIA DE ILICITUDE. PROCEDIMENTO ADMINISTRATIVO. INVIABILIDADE DE REDISCUSSÃO NO JUÍZO PENAL. MATERIALIDADE, AUTORIA E DOLO COMPROVADOS.

1. Exige o crime de sonegação tributária conduta ativa ou de relevante omissão para a consciente supressão - total ou parcial - de tributos. Verifica-se perfeitamente a subsunção do comportamento à norma incriminadora, afrontando o bem jurídico protegido pelo tipo legal.

2. Não configura cerceamento de defesa a intimação do acusado para especificar os fatos que pretende demonstrar com a prova testemunhal, haja vista a necessidade de o julgador, destinatário direto da prova, avaliar a necessidade da oitiva, nos termos do artigo 400, §1º, do Código de Processo Penal.

3. O fato de a denúncia estar embasada em dados bancários e fiscais obtidos e repassados diretamente pela Receita Federal por meio do compartilhamento de informações, sem qualquer intervenção judicial, não representa qualquer ilegalidade, conforme decidiu o e. STF por ocasião do julgamento do Recurso Especial nº 1.055.941/SP, submetido à repercussão geral (Tema nº 990).

4. A jurisprudência dominante manifesta-se no sentido de que eventuais vícios na constituição do crédito tributário são, em princípio, examináveis na competente via administrativa e/ou cível (âmbito judicial), não competindo ao juízo criminal imiscuir-se na matéria.

5. No delito previsto no artigo 1º da Lei nº 8.137/1990, o dolo é genérico. Sendo prescindível um especial fim de agir, o elemento subjetivo decorre da intenção de suprimir o pagamento de tributos, o que restou, à evidência da materialidade e da autoria delitivas, demonstrado na espécie.

6. Comprovados a materialidade, a autoria e o dolo, e ausentes causas excludentes da ilicitude ou da antijuridicidade, impõe-se a manutenção da condenação do réu pela prática do delito previsto no artigo 1º, I e II, da Lei nº 8.137/90. (TRF4, ACR 5018683-62.2012.4.04.7200, SÉTIMA TURMA, Relator LUIZ CARLOS CANALLI, juntado aos autos em 17/03/2020)

Link: https://jurisprudencia.trf4.jus.br/pesquisa/citacao.php?doc=TRF421144755

**HC 5049748-97.2019.4.04.0000**

EMENTA: HABEAS CORPUS. CRIMES CONTRA O SISTEMA FINANCEIRO NACIONAL. DEFERIMENTO DO PEDIDO DE BUSCA E APREENSÃO. ILEGALIDADE. NÃO OCORRÊNCIA.

1. É assente na jurisprudência dos Tribunais Superiores o entendimento no sentido da necessidade de racionalização do writ, a fim de que seja observada a sua função constitucional de sanar ilegalidade ou abuso de poder que resulte coação ou ameaça à liberdade de locomoção do paciente. Por tal motivo, não se admite a impetração de habeas corpus em substituição ao recurso próprio (apelação, agravo de execução, recurso especial) ou à revisão criminal, ressalvados os casos em que presente flagrante ilegalidade em prejuízo da liberdade do paciente.

2. A jurisprudência do Superior Tribunal de Justiça tem sido flexível em alguns casos, em que as impetrações não se afeiçoam à defesa do direito de ir e vir, mas apontam, ainda que em tese, a existência de flagrante ilegalidade.

3. Caso em que não se verifica a existência de flagrante ilegalidade a ensejar a excepcional concessão da ordem, uma vez que a decisão se encontra devidamente fundamentada, com a exposição dos motivos que levaram ao deferimento da medida de busca e apreensão.

4. O fato de o pedido de busca e apreensão ter decorrido de informações obtidas pela Polícia Federal por meio do compartilhamento de informações pela Receita Federal do

Brasil e pelo Conselho de Controle de Atividades Financeiras - COAF (Unidade de Inteligência Financeira - UIF), sem qualquer intervenção judicial, não representa qualquer ilegalidade, conforme decidiu o e. STF por ocasião do julgamento do RE nº 1.055.941/SP, submetido à repercussão geral (Tema nº 990).

5. Ordem de habeas corpus denegada. (TRF4, HC 5049748-97.2019.4.04.0000, SÉTIMA TURMA, Relator LUIZ CARLOS CANALLI, juntado aos autos em 28/01/2020)

Link:https://jurisprudencia.trf4.jus.br/pesquisa/citacao.php?doc=TRF420738196

**ACR 5011505-08.2016.4.04.7205**

EMENTA: PROCESSO PENAL. AGRAVO REGIMENTAL. DADOS BANCÁRIOS. RECEITA FEDERAL DO BRASIL. COMPARTILHAMENTO. AUSÊNCIA DE ORDEM JUDICIAL. TEMA 990. JULGAMENTO STF. RECURSO PREJUDICADO

1. Embora a redação do Tema nº 990 pudesse parecer de certa forma abrangente, o debate travado no Supremo Tribunal Federal concentrava-se no compartilhamento de dados bancários obtidos, independentemente de ordem judicial, com base nas hipóteses da Lei Complementar nº 105/2001, o que não inclui o fornecimento das movimentações bancárias pelo próprio contribuinte no curso do procedimento fiscal.

2. No julgamento do Recurso Extraordinário nº 1055941, em regime de Repercussão Geral, o Plenário do Supremo Tribunal Federal, revogou a liminar que determinava a suspensão dos processos e fixou a tese considerando constitucional o compartilhamento dos relatórios de inteligência financeira da UIF e da íntegra do procedimento fiscalizatório da Receita Federal do Brasil, que define o lançamento do tributo, com os órgãos de persecução penal para fins criminais, sem a obrigatoriedade de prévia autorização judicial, devendo ser resguardado o sigilo das informações em procedimentos formalmente instaurados e sujeitos a posterior controle jurisdicional, sendo que tal compartilhamento deve ser feito unicamente por meio de comunicações formais, com garantia de sigilo, certificação do destinatário e estabelecimento de instrumentos efetivos de apuração e correção de eventuais desvios. (TRF4, ACR 5011505-08.2016.4.04.7205, SÉTIMA TURMA, Relatora SALISE MONTEIRO SANCHOTENE, juntado aos autos em 19/12/2019).



Link: https://jurisprudencia.trf4.jus.br/pesquisa/citacao.php?doc=TRF420605429

**AC 5001183-57.2015.4.04.7109**

EMENTA: APELAÇÃO CÍVEL. ADMINISTRATIVO. SERVIÇO DE TELEFONIA. COMPETÊNCIA DA JUSTIÇA FEDERAL. LEGITIMIDADE DO MINISTÉRIO PÚBLICO FEDERAL. VIOLAÇÃO A DIREITO DO CONSUMIDOR. DÚVIDA. APRESENTAÇÃO DE LISTAGEM COMPLETA DE TODOS OS CONSUMIDORES DE SERVIÇO DE INTERNET NO MUNIÍPIO DE BAGÉ/RS. PROTEÇÃO AO SIGILO ESTABELECIDO NA CONSTITUIÇÃO FEDERAL (ART. 5º, X E XII). LEI Nº 9.472/1997 (ARTIGO 3º, V E IX, E ARTIGO 72). JULGAMENTO SEGUNDO PROCEDIMENTO DO ARTIGO 942 DO CPC.

1. A competência da Justiça Federal decorre do fato de o Ministério Público Federal ser autor desta ação.

2. É inequívoca a legitimidade ativa do Ministério Público Federal, cuja atuação, como visto, tem por objetivo, dentre outras, a proteção de direitos individuais homogêneos, de origem comum (CDC, art. 81, III), contribuindo para evitar que cada consumidor tenha que, individualmente, promover sua própria demanda.

3. A Constituição de 1988, no artigo 5º, incisos X e XII, assegura a inviolabilidade da intimidade, da vida privada das pessoas e das comunicações telefônicas e de dados. No mesmo sentido, o artigo 3º, incisos V e IX e artigo 72, da Lei 9.472/1997, asseguram ao usuário de serviços de telecomunicações, o direito à inviolabilidade e ao segredo de sua comunicação e ao respeito de sua privacidade.

4. A pretensão do Ministério Público Federal reside em apurar eventual hipótese de dano patrimonial, decorrente de suposta violação a direito consumerista. Os dados necessários podem ser obtidos diretamente com os assinantes que, assim, autorizam a divulgação dos seus dados pertinentes. A matéria é sempre sensível. Embora não se cogite da violação de conversas, há risco de exposição da privacidade dos assinantes. (TRF4, AC 5001183-57.2015.4.04.7109, TERCEIRA TURMA, Relatora MARGA INGE BARTH TESSLER, juntado aos autos em 16/10/2019.

Link: https://jurisprudencia.trf4.jus.br/pesquisa/citacao.php?doc=TRF420081621

**ACR 5013569-69.2017.4.04.7200**

EMENTA: PROCESSO PENAL. EMBARGOS DE DECLARAÇÃO EM APELAÇÃO. DECISÃO QUE IMPÔS MULTA SANCIONATÓRIA POR DESCUMPRIMENTO DE DECISÃO JUDICIAL. INTERCEPTAÇÃO DO FLUXO DE COMUNICAÇÕES VIA APLICATIVO WHATSAPP DETERMINADA NO BOJO DE INVESTIGAÇÃO CRIMINAL (OPERAÇÃO "SIMON"). OMISSÃO CARACTERIZADA. LEGITIMIDADE DA EMPRESA FACEBOOK PARA CUMPRIMENTO DA ORDEM JUDICIAL. OBSCURIDADE E CONTRADIÇÃO NÃO VERIFICADAS. PROVIMENTO PARCIAL DOS ACLARATÓRIOS. MANTIDO O RESULTADO DO JULGAMENTO DAS APELAÇÕES.

1. Deve ser sanada a omissão relativa à legitimidade da Facebook Serviços Online do Brasil Ltda. para cumprimento da ordem judicial, não obstante a autonomia entre a aludida empresa e a WhatsApp Inc.. A ordem de interceptação do fluxo das comunicações do aplicativo WhatsApp de investigados foi direcionada à empresa Facebook Serviços Online do Brasil, com fundamento no art. 11 do Marco Civil da Internet. O artigo 12 da mesma lei prevê a aplicação de sanções decorrentes de descumprimento das normas estabelecidas nos artigos 10 e 11. No inciso II do referido dispositivo legal, a lei se vale do conceito de grupo econômico, quando prevê punições.

2. Não obstante a interceptação das comunicações do aplicativo WhatsApp devesse ser implementada pela empresa WhatsApp Inc., localizada no exterior e sem representação jurídica no Brasil, restou evidenciado que a ordem judicial foi dirigida à Facebook Serviços Online do Brasil Ltda., por ser empresa sediada em território nacional que integra o mesmo grupo econômico. Na solicitação de informações a grupos empresariais, o Poder Judiciário, diante da urgência e gravidade dos fatos criminosos que almejava evitar e esclarecer, pode exigir que a informação seja prestada por pessoa jurídica situada no Brasil, a qual detém conhecimentos suficientes para encaminhar a decisão judicial para o pronto atendimento pelo setor competente ou por outra empresa pertencente ao conglomerado, localizada em território estrangeiro. Assim, sendo a Facebook Serviços Online do Brasil Ltda. a representante no país do grupo empresarial Facebook Inc., o qual engloba o WhatsApp Inc., possui legitimidade para responder pelo serviço de comunicações no Brasil pelas operações do aplicativo WhatsApp. Precedentes. Logo, cabe à Facebook Serviços Online do Brasil Ltda. o pagamento da multa imposta.

3. Relativamente à alegação de impossibilidade técnica e material de cumprimento da decisão judicial, verifica-se que o voto condutor, ao fazer considerações sobre o direito constitucional à livre iniciativa e a preservação e entrega de conteúdo das conversas realizadas via aplicativo WhatsApp, entendeu que não pode esta Corte, no caso concreto, afastar a ordem judicial, cabendo à empresa interessada interceder, perante o Poder Legislativo ou o Supremo Tribunal Federal, pleiteando o afastamento da exigência em comento.

4. Alguns excertos do laudo pericial, elaborado no âmbito da ACR nº 5003809-05.2017.4.04.7004, julgada pela Oitava Turma, aventam sobre a possibilidade do cumprimento da ordem judicial, mediante o desenvolvimento de meios de capturar o código fornecido para habilitação do Whatsapp WEB, utilizando-o para fins de espelhamento, com autorização judicial.

5. O julgado embargado menciona expressamente que a medida encontra respaldo no art. 12, II, da Lei nº 12.965/2014 (Marco Civil da Internet) e nos arts. 536 e 537 do Código de Processo Civil, aplicados supletivamente, conforme disposto no artigo 3º do CPP.

6. O voto condutor faz a distinção entre o contempt of court de natureza processual civil e o de natureza processual penal, concluindo que este último constitui meio de coerção revestido de caráter preventivo e punitivo, cujo objetivo não é apenas penalizar ato atentatório à dignidade da justiça, mas coibir futuros descumprimentos de ordem emanadas pelo Juízo criminal e preservar a eficácia de suas decisões. Logo, não há falar em limitação do valor da sanção pecuniária, a qual, aliás, foi reduzida pela Turma julgadora em um décimo do valor imposto pela magistrada de origem.

7. Embargos parcialmente providos, a fim de suprir omissão, mantendo, contudo, o resultado do julgamento do apelo. (TRF4, ACR 5013569-69.2017.4.04.7200, SÉTIMA TURMA, Relator MARCOS CÉSAR ROMEIRA MORAES, juntado aos autos em 10/10/2019).

Link: **https://jurisprudencia.trf4.jus.br/pesquisa/citacao.php?doc=TRF420009528**

**COR 2009.04.00.023525-0**

EMENTA: PENAL. CORREIÇÃO PARCIAL. FORNECIMENTO DE DADOS CADASTRAIS DE CORRENTISTAS. AUTORIZAÇÃO JUDICIAL. DESNECESSIDADE.

1. O sigilo bancário abrange apenas as "operações ativas e passivas e os serviços prestados", conforme dispõe o art. 1º da Lei Complementar nº 105/2001, desta forma não incluindo os dados cadastrais de correntistas, entendidos como o nome, endereço, telefone, RG ou CPF (ou CNPJ).

2. Os elementos cadastrais revestem-se de natureza objetiva, e estão relacionadas com o próprio exercício da cidadania e, via de regra, não se encontram acobertados pela esfera de proteção do art. 5º, X e XII, da Constituição Federal. (TRF4, COR 2009.04.00.023525-0, SÉTIMA TURMA, Relator TADAAQUI HIROSE, D.E. 05/08/2009).

Link: **https://jurisprudencia.trf4.jus.br/pesquisa/citacao.php?doc=TRF400182809**

**ACR 5014165-82.2019.4.04.7200**

EMENTA: PROCESSO PENAL. INVESTIGAÇÃO CRIMINAL. FACEBOOK E WHATSAPP. QUEBRA DE SIGILO. EMPRESA CONTROLADORA ESTRANGEIRA. DADOS ARMAZENADOS NO EXTERIOR. MULTA. COERCITIVIDADE. EFETIVIDADE DAS DECISÕES JUDICIAIS. CONTEMPT OF COURT. MARCO CIVIL DA INTERNET. LEGIMITIDADE DE TERCEIROS. PARÂMETROS DA SANÇÃO PROCESSUAL. MARCO TEMPORAL. META DADOS. OBRIGATORIEDADE DE FORNECIMENTO. INEXISTÊNCIA DE DESCUMPRIMENTOS DAS ORDENS JUDICIAIS NO CASO CONCRETO. AFASTAMENTO DA MULTA.

1. Determinada a quebra de sigilo telemático em investigação de crime cuja apuração e punição sujeitam-se à legislação brasileira, impõe-se ao impetrante o dever de prestar as informações requeridas, mesmo que os servidores de dados da empresa se encontrem em outro país, uma vez que se trata de empresa constituída conforme as leis locais e, por este motivo, sujeita tanto à legislação brasileira quanto às determinações da autoridade judicial brasileira.

2. O armazenamento de dados no exterior não obsta o cumprimento da medida que determinou o fornecimento de dados telemáticos, uma vez que basta à empresa controladora estrangeira repassar os dados à empresa controlada no Brasil, não ficando caracterizada, por esta transferência, a quebra de sigilo.

3. Nos termos do Marco Civil da Internet, é lícita a transmissão de mensagens criptografadas, assim como a utilização da tecnologia ponta a ponta e o protocolo Signal, não estando as empresas de telecomunicações obrigadas a modificar seus produtos para criação de meios de interceptação, como a introdução de backdoor, men-in-the-middle (MITM), espelhamento são providências que importam em modificação do produto (aplicativo) e que implicam em fragilização de sua segurança do serviço.

4. Isso, porém, não as desobriga do dever de prestar ao Poder Judiciário as informações que lhe forem requisitas e sejam tecnicamente possíveis fornecer, como metadados e mensagens criptografadas, o que não ocorreu, mesmo após dezoito meses e sucessivas ordens judiciais.

5. É imperioso que as empresas de telecomunicações, mesmo sem modificar seus produtos, auxiliem as autoridades judiciais na solução de crimes, inclusive com a apresentação de apresentando alternativas viáveis e ferramentas tecnológicas aptas à prevenção.

6. A decisão relativa ao local de armazenamento dos dados é questão de âmbito organizacional interno da empresa, não sendo de modo algum oponível ao comando judicial que determina a quebra de sigilo.

7. O legislador pátrio não descurou da necessidade de, além das próprias partes, também direcionar medidas coercitivas em face de terceiros não integrantes da relação processual penal ou mesmo de tipificar condutas como, por exemplo, o crime de desobediência (art. 330 do CP).

8. É lícita a fixação de penalidade em face de descumprimento de ordem judicial. Hipótese em que a imposição de multa sancionatória não visa à indenização da parte ou à expropriação do devedor, tendo, ao revés, a pretensão de assegurar a necessária força imperativa das decisões judiciais, sob pena de tornar inócua e ineficiente a tutela do processo e dos interesses públicos envolvidos. Hipótese em que tem maior afeição com o contempt of court do Direito Anglo-Saxônico, do que propriamente com o regime jurí-

dico que o Novo Código de Processo Civil fixou para astreintes, notadamente em razão do fixado no art. 144-A do Código de Processo Penal.

9. A sujeição da efetivação da multa por descumprimento de decisão judicial ao processo executivo implica em subversão lógica e violação ao princípio da efetividade da jurisdição, notadamente porque a ordem não atendida pelo impetrante não é suscetível de cumprimento por outrem ou satisfação por meio diverso.

10. A multa tem lugar quando a parte a quem é dirigida a ordem deixa de cumpri-la ou a cumpre com atraso injustificado, não sendo relevante a mera alegação de dificuldades operacionais, em especial diante da contumaz negativa da impetrante de submeter-se à jurisdição nacional. Caso em que a majoração escalonada da multa por descumprimento é inerente à sequência das decisões judiciais reiteradamente descumpridas ao longo de dezoito meses.

11. A aplicação da multa por descumprimento, no caso, não se submete aos parâmetros e limites previstos na legislação civil, tampouco ao processo executivo, devendo-se ter como termo final, contudo, a data do oferecimento da denúncia, pois, em princípio, no momento da instauração da ação penal, a diligência descumprida não mais se mostra necessária.

12. O bloqueio, como medida coercitiva, não suprime da parte o acesso à justiça ou aos meios legais disponíveis para defender-se; não se sujeita, porém, como pretendido, ao prévio processo executivo, porquanto não consentâneo com sua natureza e finalidade.

13. Devidamente intimada a empresa da decisão judicial que lhe advertiu das consequências do descumprimento da ordem, oportunidade em que a autoridade apontada como coatora lhe facultou prestar informações sobre eventual impossibilidade de cumprimento, alcançando-lhe a possibilidade de defender-se no primeiro grau, sendo-lhe assegurada, ademais, recurso ao Tribunal, não há falar em violação ao devido processo legal.

14. No presente caso, uma vez que já a partir da primeira ordem judicial houve justificativa plausível para o descumprimento da ordem, conforme restou esclarecido no laudo pericial produzido nos autos do processo paradigma - inclusive com exposição



das razões técnicas para o não fornecimento dos dados telemáticos solicitados e posteriormente oferecimento de demais informações(metadados), entendo não ter havido resistência à ordem judicial passível de sanção.

15. Provida a apelação criminal interposta pela empresa WHATSAPP Inc.

16. Prejudicadas as seguintes impugnações judiciais: Mandado de segurança nº 5001019-40.2019.4.04.0000; Mandado de segurança nº 5000026-94.2019.4.04.0000; Apelação criminal nº 50006927-12.2019.4.04.7200; Mandado de segurança nº 5046072-78.2018.4.04.0000; Mandado de segurança nº 5019861-68.2019.4.04.0000; e Reclamação nº 5021611-08.2019.4.04.0000. (TRF4, ACR 5014165-82.2019.4.04.7200, OITAVA TURMA, Relator JOÃO PEDRO GEBRAN NETO, juntado aos autos em 03/10/2019)

Link: **https://jurisprudencia.trf4.jus.br/pesquisa/citacao.php?doc=TRF419951632**

**MS 5002827-27.2012.4.04.0000**

EMENTA: PROCESSUAL PENAL. MANDADO DE SEGURANÇA. DADOS CONTIDOS EM TELEFONE CELULAR. GARANTIA CONSTITUCIONAL DA INTIMIDADE. AUTORIZAÇÃO JUDICIAL. IMPRESCINDIBILIDADE. É cabível o afastamento do sigilo telefônico e telemático, determinado em decisão judicial fundamentada, em hipóteses legalmente previstas, especialmente quando há crimes com impossibilidade de investigação por outra maneira. Se o acesso aos dados sigilosos contidos na memória de telefone celular, constantes no laudo elaborado pela Autoridade Policial, se deu sem autorização judicial, impõe-se o seu desentranhamento dos autos. (TRF4 5002827-27.2012.4.04.0000, SÉTIMA TURMA, Relator MÁRCIO ANTÔNIO ROCHA, juntado aos autos em 28/08/2012).

Link: **https://jurisprudencia.trf4.jus.br/pesquisa/citacao.php?doc=TRF402986253**

**AMS 2005.72.00.013027-1**

EMENTA: APELAÇÃO. MANDADO DE SEGURANÇA. PROCESSUAL PENAL. EMPRESA DE TELEFONIA. DADOS CADASTRAIS DE CLIENTES. REQUISIÇÃO. AUTORIDADE POLICIAL. ART. 5º, XII, DA CF. SIGILO. QUEBRA. AUTORIZAÇÃO JUDICIAL. NECESSIDADE.

1. Tem legitimidade para impetrar o mandamus a companhia telefônica que, ao reputar ilegal a ordem emanada pela Polícia Federal, para que forneça dados cadastrais de seus clientes, pretende ver reconhecido perante o Poder Judiciário seu direito líquido e certo de não prestar as informações solicitadas.

2. O sigilo telefônico incide não apenas sobre as comunicações telefônicas propriamente ditas (regulamentada pela Lei nº 9.296/96) mas também sobre os respectivos dados e registros, constituindo projeção específica do direito à privacidade garantido na Lei Maior.

3. Referido direito fundamental não pode ser tido como absoluto, tendo em vista a natural restrição resultante do princípio da convivência das liberdades.

4. Para evitar possíveis abusos por parte dos órgãos estatais, a quebra de sigilo deve ser feita com observância do procedimento legalmente estabelecido, ou seja, mediante autorização judicial devidamente fundamentada, sendo demonstrada a efetiva necessidade da medida restritiva.

5. Portanto, a determinação da autoridade policial para que sejam revelados dados sigilosos afigura-se ilegal, uma vez que a produção das provas pretendidas dependeria da competente autorização judicial. (TRF4, AMS 2005.72.00.013027-1, OITAVA TURMA, Relator ÉLCIO PINHEIRO DE CASTRO, DJ 25/10/2006).

Link: **https://jurisprudencia.trf4.jus.br/pesquisa/citacao.php?doc=TRF400134574**

## Comentários

As decisões tratam dos parâmetros que devem ser observados no âmbito da administração pública federal para o acesso a dados pessoais.

Ganha destaque o limite ao compartilhamento de dados principalmente em ações de execução fiscal. Resulta fixado pela jurisprudência do TRF4 que é plenamente possível o compartilhamento de dados entre os órgãos e entidades da administração pública federal, sem qualquer intervenção judicial.



Por outro lado, a administração pública não pode exigir o fornecimento de dados em poder da iniciativa privada sem autorização judicial, devendo demonstrar a necessidade da medida restritiva, sob pena de ser caracterizado abuso, e violação à intimidade. Nessa perspectiva, a coleta de provas efetuada pela Polícia Federal como regra, necessita de autorização Judicial (art. 5º, XII, CF). De acordo com a jurisprudência do TRF4 devem ser disponibilizado apenas os dados objeto da autorização judicial, sem qualquer outro dado que permita a identificação do usuário. Logo, mesmo que de forma indireta, A Corte já está a observar a premissa de dados anonimizados, na esteira do que dispõe o art. 5.º da LGPD. Nesse sentido, o fornecimento do número originador da chamada telefônica recebida não equivale a divulgação de dados cadastrais ou do conteúdo da conversa.

Como se observa a jurisprudência do TRF4 já contém esboçados os elementos de proteção do controle e do tratamento de dados, na linha do que está regulado pela LGPD, de modo que com a entrada em vigor da lei estará facilitada a sistematização das decisões da Corte, na direção de dar efetividade aos direitos regulados.

# TRATAMENTO DE DADOS PESSOAIS NA OUVIDORIA DO TJPR

## Apresentação

A Revista da Ouvidoria mostra nesta seção os procedimentos adotados no recebimento das manifestações efetuadas pelos usuários, com relevância para os procedimentos adotados na proteção de dados pessoais, antes da entrada em vigor da Lei n.º 13.709 do ano de 2018 (LGPD).

## Recebimento, categorização e processamento das manifestações

Quando recebidas no Sistema da Ouvidoria – SISOUV – as manifestações são analisadas para constatar a finalidade, bem como a resposta a ser elaborada; podem ser informações, reclamações, denúncias, elogios ou um pedido relacionado à Lei de Acesso a Informação (LAI). Por ocasião da análise, é observado também em que órgão do Tribunal de Justiça pode ser obtida a informação requerida, desde que a Ouvidoria não detenha dados ou possa efetuá-la de imediato.



### Manifestações sigilosas

Nesta primeira fase é verificado o tipo de manifestação escolhida pelo usuário – sigilosa ou não.

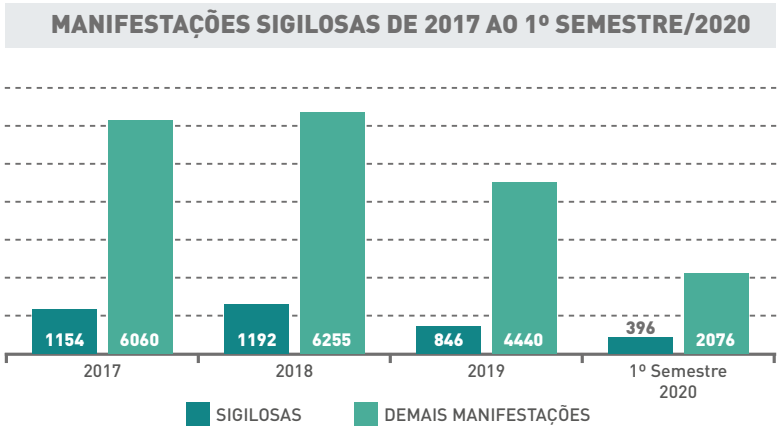
As manifestações categorizadas como sigilosas são aquelas em que o usuário, ao preencher o formulário, solicita que seus dados sejam mantidos em sigilo.

Recebida a manifestação e constatado o pedido de sigilo de dados pessoais e havendo a necessidade do envio a outras unidades administrativas ou judiciárias, omite-se os dados não disponibilizados, sendo encaminhado somente o conteúdo da manifestação.

Contudo, devido ao objeto do pedido, pode ser necessário o fornecimento dos dados pessoais do usuário para possibilitar a precisão na resposta; nestes casos, o usuário será consultado para autorizar a disponibilização de dados pessoais.

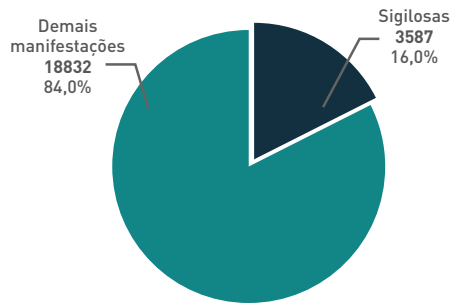
A Ouvidoria-Geral da Justiça está atenta ao propósito de preservar a vontade do manifestante acerca do pedido de sigilo em relação aos a dados pessoais, mesmo antes do advento da Lei 13.709/2018.

Segundo levantamento efetuado na Ouvidoria no ano de 2017 foram realizadas 1.154 manifestações sigilosas do total de 7.214 recebidas; em 2018, foram 1.192 do total de 7.447; em 2019, 546 do total de 5.296 e no primeiro semestre de 2020, foram recebidas 396 manifestações sigilosas do total de 2.472.



Observa-se que o montante anual dos pedidos de sigilo gira em torno de 16%, conforme exemplificado no gráfico a seguir:

**MANIFESTAÇÕES DE 2017 AO 1º SEMESTRE/2020**




## Manifestações anônimas

Na fase de categorização são identificadas as manifestações efetuadas sob anonimato.

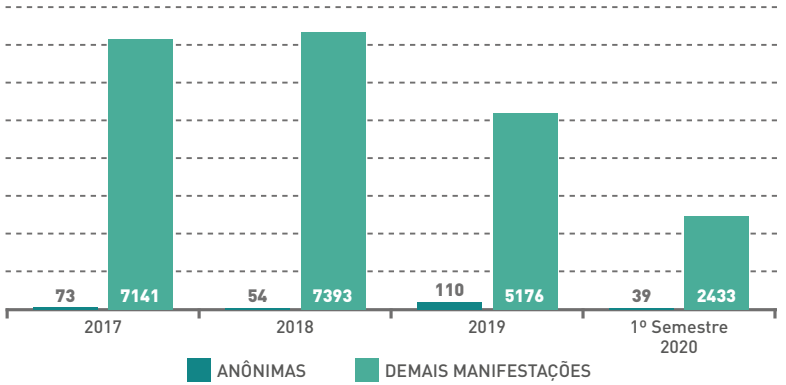
A partir de 26 de novembro de 2018, com aprovação do colendo Órgão Especial do Tribunal de Justiça da Resolução n. 212, que regulamentou a atividade da Ouvidoria-Geral do Tribunal, as manifestações realizadas de forma anônima passaram a não ser admitidas, consoante o disposto no artigo 5º, inciso I da mencionada Resolução.

O procedimento adotado com as manifestações anônimas foi o de recebê-las e, na resposta ao usuário, informar a vedação legal, sendo-lhe facultado a possibilidade de efetuar o mesmo pedido sob a forma sigilosa, garantindo-lhe a preservação de dado pessoais.

As manifestações anônimas não são expressivas ficando em torno de 1 a 2% do total recebido pela Ouvidoria-Geral; em 2017 foram recebidas 73 manifestações anônimas do total de 7.214; em 2018, 54 manifestações anônimas do total de 7.447; em 2019, 110 manifestações anônimas do total de 5.286 e no primeiro semestre de 2020, 39 manifestações anônimas do total de 2.472, conforme consta do gráfico:

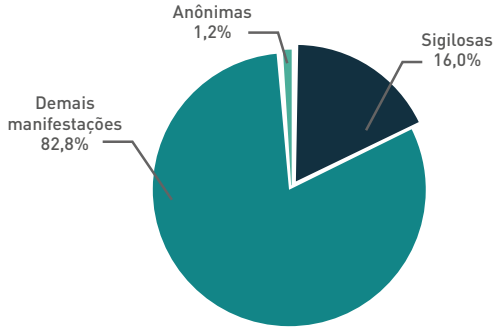


**MANIFESTAÇÕES ANÔNIMAS DE 2017 AO 1º SEMESTRE/2020**




A quantidade de manifestações sigilosas e anônimas recebidas pela Ouvidoria-Geral, no período entre 2017 e 1º semestre de 2020, está representada no gráfico abaixo:

**TIPOS DE MANIFESTAÇÕES 2017-2020**




Conforme se observa, mesmo antes da entrada em vigor da LGPD, a Ouvidoria-Geral do Tribunal de Justiça do Paraná já adota procedimentos de proteção de dados pessoais.

Desde 11 de setembro de 2020, em atendimento a Lei Geral de Proteção de Dados (Lei 13.709/2018), a Ouvidoria-Geral disponibiliza formulário de pedido de autorização do usuário para a disponibilização de dados pessoais, necessários a tramitação de manifestação no Tribunal de Justiça.

TJPR

TRIBUNAL DE JUSTIÇA
DO ESTADO DO PARANÁ