ReGeo ISSN: 2177-3246

# O JOGO DE DADOS ENTRE O ESTADO E AS BIG TECHS: UMA ANÁLISE JURÍDICO-CONSTITUCIONAL DA SOBERANIA DIGITAL NO BRASIL

# THE HIGH-STAKES DATA GAME BETWEEN THE STATE AND BIG TECH: A LEGAL-CONSTITUTIONAL ANALYSIS OF DIGITAL SOVEREIGNTY IN BRAZIL

# EL JUEGO DE LOS DATOS ENTRE EL ESTADO Y LAS BIG TECH: UN ANÁLISIS JURÍDICO-CONSTITUCIONAL DE LA SOBERANÍA DIGITAL EN BRASIL

10.56238/revgeov16n5-303

**André Pires Gontijo**
Doutor em Direito
Instituição: Centro Universitário de Brasília (CEUB)
E-mail: andre.gontijo@ceub.edu.br, andre.gontijo@gmail.com
Orcid: https://orcid.org/0000-0003-0683-2679
Lattes: http://lattes.cnpq.br/4832720444198741

**Fernanda de Paiva Barth**
Graduanda em Direito
Instituição: Centro Universitário de Brasília (CEUB)
E-mail: fernandapaivabarth@gmail.com
Orcid: https://orcid.org/0009-0005-2084-7262
Lattes: https://lattes.cnpq.br/4082818442312733

**RESUMO**
O presente trabalho tem como objetivo analisar como a arquitetura jurídico-constitucional brasileira, no contexto do constitucionalismo multinível, responde aos desafios impostos pelas Big Techs para a afirmação da soberania digital. Por meio de uma metodologia teórico-documental, a pesquisa investiga o poder dessas empresas no tratamento de dados e na manipulação informacional. Os resultados demonstram que o ordenamento jurídico nacional, influenciado por marcos regulatórios globais como o Regulamento Geral de Proteção de Dados (GDPR), evoluiu com a promulgação da Lei geral de Proteção de Dados (LGPD) e do Marco Civil da Internet (MCI) para estabelecer a responsabilidade das plataformas. Constatou-se que a atuação das Big Techs, através do uso de algoritmos e da criação de bolhas informacionais, impacta diretamente a autonomia individual e a estabilidade democrática, como evidenciado por casos emblemáticos como o da Cambridge Analytica e a intervenção do Supremo Tribunal Federal (STF) no caso Telegram. Conclui-se que, apesar dos avanços legislativos, a capacidade do Estado brasileiro de regular efetivamente o fluxo de dados e coibir a desinformação permanece um desafio central para a proteção do processo democrático frente ao poder transnacional das gigantes de tecnologia.

**Palavras-chave:** Constitucionalismo Multinível. *Big Techs*. Soberania Digital. Proteção de Dados. Regulação da Internet.

**ABSTRACT**
This paper aims to analyze how Brazil's legal-constitutional framework, within the context of multilevel constitutionalism, responds to the challenges posed by Big Tech for the assertion of digital sovereignty. Through a theoretical-documentary methodology, the research investigates the power of these companies in data processing and information manipulation. The findings demonstrate that the national legal system, influenced by global regulatory frameworks such as the General Data Protection Regulation (GDPR), has evolved with the enactment of the General Data Protection Law (LGPD) and the Brazilian Internet Civil Rights Framework Marco Civil da Internet (MCI) to establish platform liability. It was found that the activities of Big Tech, through the use of algorithms and the creation of information bubbles, directly impact individual autonomy and democratic stability, as evidenced by landmark cases such as Cambridge Analytica and the intervention of the STF (Brazilian Supreme Federal Court) in the Telegram case. The paper concludes that, despite legislative advances, the Brazilian State's ability to effectively regulate the flow of data and curb disinformation remains a central challenge for the protection of the democratic process in the face of the transnational power of the tech giants.

**Keywords:** Multilevel Constitutionalism. Big Tech. Digital Sovereignty. Data Protection. Internet Regulation.

**RESUMEN**
El presente trabajo tiene como objetivo analizar cómo la arquitectura jurídico-constitucional brasileña, en el contexto del constitucionalismo multinivel, responde a los desafíos impuestos por las Big Tech para la afirmación de la soberanía digital. Por medio de una metodología teórico-documental, la investigación indaga sobre el poder de estas empresas en el tratamiento de datos y en la manipulación informacional. Los resultados demuestran que el ordenamiento jurídico nacional, influenciado por marcos regulatorios globales como el Reglamento General de Protección de Datos (GDPR), evolucionó con la promulgación de la Ley General de Protección de Datos (LGPD) y del Marco Civil de Internet (MCI) para establecer la responsabilidad de las plataformas. Se constató que la actuación de las Big Tech, a través del uso de algoritmos y la creación de burbujas informativas, impacta directamente la autonomía individual y la estabilidad democrática, como evidencian casos emblemáticos como el de Cambridge Analytica y la intervención del STF (Supremo Tribunal Federal) en el caso Telegram. Se concluye que, a pesar de los avances legislativos, la capacidad del Estado brasileño para regular efectivamente el flujo de datos y frenar la desinformación permanece como un desafío central para la protección del proceso democrático frente al poder transnacional de los gigantes tecnológicos.

**Palabras clave:** Constitucionalismo Multinivel. Big Tech. Soberanía Digital. Protección de Datos. Regulación de Internet.

## 1 INTRODUÇÃO

No mundo contemporâneo, as atividades pessoais e profissionais tornam-se cada vez mais dependentes do ambiente digital, impulsionadas pela evolução tecnológica. Grande parte dessas informações circula por plataformas de grandes empresas de tecnologia, conhecidas como Big Techs.

Dessa forma, os direitos fundamentais, especialmente a proteção de dados pessoais, ganharam relevância significativa no sistema jurídico atual. Pois, vive-se em um contexto do constitucionalismo multinível, que transcende o Estado Nacional e considera as interações entre diferentes níveis jurídicos e a posição do indivíduo nessa estrutura.

Assim, legislações estrangeiras que protegem dados têm influência global. O Regulamento Geral sobre a Proteção de Dados (GDPR) da União Europeia, implementado em 2018, foi um marco que mudou a abordagem global da proteção de dados, inspirando leis similares no Brasil, como a Lei Geral de Proteção de Dados (LGPD), Marco Civil da Internet (MCI) e o projeto de lei PNCiber/SNCiber. O Estado brasileiro busca responsabilizar empresas pela proteção de dados, viabilizando segurança jurídica aos usuários. A justificativa para esse ensaio, reside na importância de abordar questões acerca do impacto tecnológico no que se refere a proteção e segurança no tratamento desses dados em um novo mundo totalmente hiperconectado e de livre acesso.

Nessa perspectiva, a problemática do presente trabalho de conclusão de curso consiste em responder à seguinte questão: considerando a crescente influência das Big Techs no "jogo de dados" global, como a arquitetura jurídico-constitucional brasileira, no contexto do constitucionalismo multinível, responde aos imperativos de afirmação da soberania digital, especialmente no que tange à capacidade do Estado de regular o tratamento de dados e coibir a manipulação informacional que ameace a autonomia individual e a estabilidade democrática?

A partir disso, a hipótese inicial de pesquisa reside em uma visão positiva, em que a estrutura jurídico-constitucional brasileira tem reagido de forma proativa aos imperativos da soberania digital por meio de marcos como o Marco Civil da Internet e a LGPD. Apesar desses avanços na regulação de dados e plataformas, permanece a necessidade constante de compreender mais profundamente as dinâmicas digitais e as implicações decorrentes do poder das grandes empresas de tecnologia.

O problema de pesquisa aborda o crescente poder de empresas como Google, Meta, Apple e Microsoft, que não são apenas provedoras de serviços, mas também coletoras, processadoras, analistas e monetizadoras de dados, influenciando comportamentos, mercados e discursos públicos.

Logo, o presente estudo também disserta sobre a eficácia da regulação brasileira, especialmente com a LGPD, no tratamento de dados pessoais, e investiga a capacidade do Estado de combater a manipulação informacional que ameaça a autonomia individual e a estabilidade democrática, tais como a desinformação e a influências em processos eleitorais.

Ademais, a pesquisa terá como objetivo geral descobrir de que maneira as Big Techs

influenciam a política de soberania digital no Brasil. Constituem objetivos específicos: (i) descrever o atual cenário da política de soberania digital no Brasil; (ii) analisar o impacto das Big Techs na legislação brasileira de proteção de dados e, por fim, (iii) exemplificar a influência que as Big Techs detêm no controle de dados pessoais.

Desse modo, para melhor explanação das ideias já apresentadas, este ensaio acadêmico será dividido em três tópicos que seguem a introdução: (i) O constitucionalismo multinível e o poder das Big Techs: desafios regulatórios no Brasil; (ii) Manipulação de dados e influência eleitoral: a atuação das Big Techs e os limites constitucionais no Brasil (iii) Casos emblemáticos de como a manipulação de dados pelas Big Techs impacta o processo eleitoral.

Por fim, para o desenvolvimento do presente artigo, o procedimento metodológico empregado foi realizado com base em uma pesquisa teórica/documental utilizando artigos, sites, livros, legislações, doutrinas e vídeos relacionados ao tema, além de utilizar como auxílio ferramentas de apoio como o uso de tecnologias avançadas. As fontes e a análise dos dados empregados visam à pesquisa qualitativa, uma vez que são predominantemente textuais e conceituais. A metodologia deste artigo foi uma combinação de duas vertentes metodológicas, com um forte componente crítico-metodológico, utilizando a jurídico-dogmática como base para a análise do arcabouço normativo.

## 2 O CONSTITUCIONALISMO MULTINÍVEL E O PODER DAS *BIG TECHS*: DESAFIOS REGULATÓRIOS NO BRASIL

### 2.1 DEFINIÇÃO DE CONSTITUCIONALISMO MULTINÍVEL

O constitucionalismo multinível fundamenta-se na proteção dos direitos humanos, inserindo-se no sistema jurídico em um contexto global marcado por constantes transformações, e considerando as repercussões dessas mudanças nos diferentes ordenamentos jurídicos internos dos países. Para Pérez Conchillo (2020, p. 232) "[...] a relação entre o direito de acesso à informação pública e o constitucionalismo multinível permitirá a criação de novos cenários de proteção de direitos e a discussão de questões de inter-relação entre diferentes ordenamentos jurídicos"[1]

A partir disso, no cenário das evoluções contemporâneas, impulsionadas pelos avanços tecnológicos e o crescimento da regulação dos dados pelas *Big Techs,* os direitos humanos tornaram-se uma preocupação central nos sistemas jurídicos de diversas nações, com ênfase na proteção de dados pessoais. Conforme explicita Ley (2007, p. 279) "o constitucionalismo além do Estado se preocupa com a relação entre vários níveis jurídicos e a posição do indivíduo em um sistema jurídico

[1] Conforme no original, tradução livre de: "De tal modo, la relación derecho de acceso a la información pública-constitucionalismo multinivel permitirá plantear nuevos escenarios en la protección de los derechos y discutir cuestiones de encaje entre los distintos ordenamientos."

multinível"[2]. Visando assim, um esforço global e regional coordenado, no qual os direitos humanos são protegidos não apenas por normas internas, mas também por compromissos internacionais que buscam garantir a dignidade humana em um contexto mais amplo e abrangente rumo à universalização da proteção dos direitos fundamentais.

Nesse sentido, a forma de organização jurídica de um país, levando em conta o constitucionalismo multinível, vai além do sistema normativo que ela representa, pois dá origem a novas formas de organização político-jurídica em níveis mundial e regional, impactando os Estados e suas estruturas. "Portanto, na visão de Oliveira e Moreira (2023, p.289) rejeitando a ideia de uma pirâmide hierárquica, o Constitucionalismo Multinível [...] exige que as ordens jurídicas se comuniquem por meio do mecanismo do diálogo interjurisdicional"[3]

Com base nessas informações, serve como exemplo o Regulamento Geral sobre a Proteção de Dados (GDPR) da União Europeia (UE). Embora a GDPR seja um regulamento da UE, ele tem alcance global, pois afeta qualquer organização que processe dados de cidadãos da UE, independentemente de onde a organização esteja localizada. Ele estabelece padrões elevados para a proteção de dados pessoais e serve como um modelo para outras legislações de proteção de dados em todo o mundo. A GDPR tem como objetivo estabelecer "[...] regras relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e regras relativas à livre circulação de dados pessoais"[4] (União Europeia, 2018) e "[...] protege os direitos e liberdades fundamentais das pessoas singulares e, em particular, o seu direito à proteção de dados pessoais"[5] (União Europeia, 2018). Desse modo, esse fenômeno gera a definição de "multinível", que reflete a cooperação entre diferentes esferas normativas e jurídicas em níveis internos e externos dos países.

Ademais, para que se entenda de forma aprofundada, o constitucionalismo multinível envolve pelo menos quatro esferas de proteção dos direitos humanos conforme estabelecido por Cruz (2019, tradução nossa, grifo nosso). A primeira esfera é analisada em nível Local/Interno: a proteção dos direitos humanos no âmbito dos entes federativos, como os estados brasileiros, que possuem suas próprias Constituições Estaduais. O segundo é o nível Federal/Nacional: a Constituição e os tratados nacionais que são aplicáveis a todo o território do país, a exemplo da Constituição Brasileira de 1988. Outro Nível a ser considerado, é o Supranacional: sistemas universais e regionais (de cada continente) de proteção dos direitos humanos, como as Nações Unidas e a Organização dos Estados Americanos

[2] Conforme no original, tradução livre de: "Constitutionalism beyond the state concerns itself with the relation among various legal levels and the position of the individual in a multilevel legal system."
[3] Conforme no original, tradução livre de: "Luego, rechazando la idea de una pirámide [...] el Constitucionalismo Multinivel Interamericano requiere que las ordenes jurídicas conversen por intermedio del mecanismo del diálogo interjurisdiccional"
[4] Conforme no original, tradução livre de: "This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data."
[5] Conforme no original, tradução livre de: "This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data."

(OEA), que incluem a Comissão e o Tribunal Interamericano de Direitos Humanos. Por fim, o nível Transversal, em que há a proteção dos direitos humanos de forma coordenada entre os sistemas jurídicos de diferentes países, criando uma rede de defesa que transcende as fronteiras nacionais.

Mediante o exposto, o constitucionalismo multinível permite uma maior integração entre os diferentes sistemas de proteção dos direitos humanos, criando um sistema que busca maior eficácia e maior fiscalização sobre o cumprimento desses direitos em diversos níveis de governo e jurisdição. Pois, possibilita o fortalecimento da rede de garantias que atua tanto em nível nacional quanto internacional, assegurando que os direitos fundamentais dos indivíduos sejam respeitados e protegidos por um sistema de camadas que transcende fronteiras (nível transversal).

## 2.2 A INFLUÊNCIA DAS GIGANTES DA TECNOLOGIA NA PRIVACIDADE E SEGURANÇA DE DADOS, COM A GDPR ATUANDO COMO MARCO REGULATÓRIO E SUA INFLUÊNCIA NA LGPD E LEGISLAÇÕES CORRELATAS

Conforme assinala Battisti (2023, p.72) "as interações econômicas e sociais ocorrem por intermédio de uma infraestrutura digital que é globalmente interconectada". Grande parte da formação dessa grande rede de troca de informações é realizada por meio da utilização de plataformas e sistemas oferecidos pelas grandes empresas de tecnologia conhecidas como *Big Techs*. O termo *Big Techs* tem sua origem nos Estados Unidos, caracterizado pelo dicionário inglês *Collins English Dictionary* como substantivo "usado para descrever as maiores empresas de tecnologia"[6]. Desse modo, empresas como a Google, Meta e Microsoft fazem parte dessa denominação.

De acordo com o entendimento do Procurador Federal da Advocacia-Geral da União, Sanctis Júnior (2024, p.75):

> Essas plataformas passaram a ser, portanto, o instrumento para a realização de atos e negócios jurídicos fundamentais à própria existência do indivíduo como sujeito de direitos. Por meio delas, celebram-se contratos, efetuam-se pagamentos, formulam-se requerimentos ao Poder Público, exercita-se a liberdade de expressão.

Nessa linha, a "[...] coleta massiva de dados sobre os usuários, seja por meio de pesquisas na web, interações em redes sociais, compras online, dispositivos conectados ou outras fontes, é uma prática comum das *Big Techs*" (Pereira, 2024, p.16).

A ascensão das gigantes de tecnologia, *Big Techs*, transformou radicalmente a sociedade, a economia e a forma como interagimos, tornando-se onipresentes, moldando o ecossistema digital (Cavallaro, 2021).

Conforme aponta o autor, Saulo Nunes de Carvalho Almeida (2023), a crescente imersão social em tecnologias inovadoras e a consequente rápida transformação das relações exigem o enfrentamento

[6] Conforme o original: Big Tech is used to refer to the biggest technology companies.

dos desafios da segurança e da proteção das informações digitais. Este desafio no cenário brasileiro foi reconhecido com a criação de um projeto de lei para instituir a Política Nacional de Cibersegurança (PNCiber) e o Sistema Nacional de Cibersegurança (SNCiber). A PNCiber busca unificar a "colcha de retalhos" regulatória existente no país e minimizar os crescentes incidentes que geram prejuízos para a sociedade brasileira, assim, visa à conformidade com as melhores práticas político-institucionais mundiais, como a diretiva NIS2 da União Europeia (legislação de segurança cibernética da UE), demonstrando a importância de adaptar modelos internacionais à realidade jurídica, política e cultural nacional (Brasil, 2023). Já a criação da Agência Nacional de Cibersegurança (ANCiber), reflete a necessidade de um órgão central para coordenar e fiscalizar a cibersegurança no país, similar ao modelo europeu (Brasil, 2023).

Em virtude das informações apresentadas, o Regulamento Geral sobre a Proteção de Dados (GDPR), implementado pela União Europeia em 2018, foi um marco regulatório que acarretou uma virada significativa na abordagem global sobre como os dados pessoais devem ser coletados, processados e protegidos.

Nesse sentido, as *Big Techs* sentiram particularmente o peso dessa legislação, uma vez que seus modelos de negócio são intrinsecamente ligados à coleta e análise massiva de dados de usuários, como discutido anteriormente. Com isso, o impacto da GDPR sobre essas gigantes se manifesta de várias formas interligadas. A título de exemplo, dispõe sobre os Princípios relativos ao tratamento de dados pessoais em seu Art 5° que estabelece os princípios fundamentais como licitude, lealdade, transparência, limitação das finalidades, minimização dos dados, exatidão, entre outros.

A transparência também se tornou um pilar, exigindo que as empresas informassem claramente quais dados coletam, por que, por quanto tempo os armazenam e com quem os compartilham (União Europeia, 2018, tradução nossa).

A GDPR alterou profundamente a dinâmica entre as *Big Techs* e os usuários, pois impôs maior transparência, responsabilidade e controle sobre os dados pessoais, ao mesmo tempo em que introduziu um regime de fiscalização rigoroso.

Segundo Cavallaro (2021), o Regulamento Geral de Proteção de Dados (GDPR) constitui um marco regulatório fundamental por ser a primeira legislação específica e de ampla aplicação para a proteção de dados. Um dos impactos mais notáveis da GDPR é sua influência global. O regulamento europeu estabeleceu um padrão de referência para a proteção de dados em todo o mundo, inspirando legislações similares em outras jurisdições, como a Lei Geral de Proteção de Dados (LGPD) no Brasil. Isso pressionou as *Big Techs* a adotarem práticas de privacidade mais consistentes e específicas em suas operações globais considerando a regulação das regiões em que elas atuam.

Vale destacar que a LGPD entrou em vigência no Brasil em 2020, e assim como a GDPR seu principal objetivo é de regular e proteger os dados fornecidos pelos usuários através de princípios inspirados na GDPR.

Assim, a LGPD visa atribuir responsabilidade às empresas na proteção dos dados para que seja possível a garantia da segurança jurídica aos usuários, haja vista que a formulação de regulamentos que possam ser implementados de modo justo e efetivo depende da capacidade de advogados e legisladores em assimilar as especificidades e a natureza complexa dos dados, visto que, há obstáculos frente à ausência de uniformidade de regulação em diferentes jurisdições para implementar normas globais (Regulação [...], 2024). Nessa linha, a PNCiber, ao propor a criação do Sistema Nacional de Cibersegurança (SNCiber), busca integrar agentes públicos e privados na proteção do ciberespaço, visando uma abordagem mais coordenada e eficaz na segurança de dados no Brasil (Brasil, 2023).

Portanto, complementarmente à LGPD, a proposta da Política Nacional de Cibersegurança (PNCiber) busca unificar o panorama regulatório brasileiro, alinhar-se a práticas internacionais e instituir órgãos como a ANCiber e o SNCiber para uma gestão integrada e eficaz dos desafios da proteção de dados e cibersegurança, integrando esforços públicos e privados.

## 2.3 O DESEJO DOS ESTADOS DE CONTROLAR O AMBIENTE DIGITAL VERSUS A NATUREZA TRANSFRONTEIRIÇA DA INTERNET

As relações sociais no século XXI são em sua maioria exercidas por meio da internet, um ambiente no qual, a princípio, predomina a chamada “terra sem lei”, pois as práticas de condutas ilegais podem ser presenciadas facilmente por um usuário do ambiente digital, como comentários ofensivos, postagens que geram informações falsas e golpes exercidos por meio da chamada conta falsa. Nesse sentido, em 2021, ocorreu o “megavazamento” de dados de 223 milhões de brasileiros. O número abrange dados de falecidos. Informações expostas incluem CPF, nome, sexo e data de nascimento, além de uma tabela com dados de veículos e uma lista com CNPJs, todos esses considerados dados pessoais (Megavazamento [...], 2021). Diante de tantos crimes através da internet, surge a preocupação de haver algum tipo de regulação e garantia de segurança para os usuários que “habitam nessas terras”.

No entendimento de Carvalho, L. (2018, p. 216) “a regulação do comportamento de usuários no ambiente digital pode ser efetuada de duas formas centrais: [...] (ii) pela regulação estatal”. Dessa forma, o Estado, detentor da soberania digital, tem o dever de garantir o mínimo de proteção, no que diz respeito à segurança de dados dos usuários. Por soberania digital entende-se, conforme Carvalho, L. (2018, p. 215) pela “atuação reguladora do Estado no ambiente transfronteiriço da internet”. Assim, surge uma competição entre as *Big Techs,* que possuem grande parte da formação desses dados armazenados, e necessidade urgente do Estado em afirmar e posicionar diante do poder de controlar o fluxo de dados e garantir a aplicação de suas leis.

A Constituição Federal de 1988 prevê essa garantia de proteção dos dados no artigo 5°, incisos X e XII:

> Art. 5º da CF 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; [...] 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; (Brasil, 1988)

Assim sendo, o Estado brasileiro tem implementado soluções de aprimoramento para a proteção dessa garantia fundamental. Em 2014, entrou em vigor a Lei do Marco Civil da Internet (MCI), um passo muito importante, Soares (2020, p. 11) explica que "[...] passou a constar no seu texto legal, pela primeira vez, a palavra privacidade, dando ênfase à necessidade da proteção dos dados pessoais, consagrando-o, mais uma vez, como princípio fundamental. Essa afirmação pode ser confirmada pelo o que está disposto no Art. 8º do MCI (2014) "a garantia do direito à privacidade e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à internet".

Ademais, as tradicionais regras de aplicação da lei penal no espaço físico já não eram suficientes para regular o controle dos dados e o cometimento de crimes na internet. Dessa maneira, a solução surgiu com a chegada da Lei Geral de Proteção de Dados (LGPD). Conforme explicado por Soares (2020), LGPD terá aplicação com efeitos internacionais sempre que os dados forem coletados em território brasileiro. Isso inclui situações em que há oferta de produtos ou serviços voltados para indivíduos que se encontram no Brasil, independentemente de onde esses serviços sejam efetivamente fornecidos. A salvaguarda da LGPD abrange, assim, não só as atividades locais, mas também aquelas cujo público-alvo esteja dentro do território nacional.

Considerando isso, o art. 3º da LGPD traz o âmbito de aplicação da lei, especificando que ela se aplica a qualquer operação de tratamento de dados realizada por indivíduos ou entidades, independentemente do local de sede ou de armazenamento dos dados, desde que uma das seguintes condições seja atendida:

> I - a operação de tratamento seja realizada no território nacional;
> II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou
> III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional.
> § 1º Consideram-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta. [...]

Por fim, vale ressaltar brevemente, a importância da LGPD nos casos em que há fluxo de dados para outros lugares do mundo. Diante disso, na visão de Soares (2020, p. 22) "temos como princípios norteadores do tratamento de dados pessoais: adequação, finalidade, necessidade, livre acesso,

transparência, segurança, responsabilização e prestação de contas, prevenção, não discriminação e qualidade de dados". Portanto, esses aspectos garantem que tanto empresas nacionais quanto internacionais respeitem os direitos à privacidade dos dados dos brasileiros, concretizando o desejo do Estado de controlar o ambiente digital diante da natureza transfronteiriça da internet.

## 3 MANIPULAÇÃO DE DADOS E INFLUÊNCIA ELEITORAL: A ATUAÇÃO DAS *BIG TECHS* E OS LIMITES CONSTITUCIONAIS NO BRASIL

### 3.1 USO DE ALGORITMOS E BOLHAS INFORMACIONAIS: COMO AS REDES SOCIAIS MOLDAM A PERCEPÇÃO POLÍTICA DOS ELEITORES

A formação de bolhas sociais online é resultado de algoritmos que definem quais informações são exibidas aos usuários em redes sociais, mecanismos de busca e sites de compras, criando um confinamento informacional (Pelizzari; Barreto Junior, 2019). A esse respeito, toda vez que um usuário acessar uma rede social ou realizar uma pesquisa em um site de buscas, estará criando um perfil de influências que o manterá conectado, formando um ambiente que reflete seus desejos, vontades e percepções, moldando sua visão de mundo conforme as informações que lhe são disponibilizadas. Pelizzari e Barreto Junior (2019, p.58) afirmam que "essa referida programação informática é denominada como algoritmo, sequência de comandos formulada por analistas de sistemas computacionais e que são alimentados pelos dados dos próprios usuários". Ressalta-se que grande parte da fonte primária desses dados são gerados e armazenados pelas *Big Techs,* já que elas são um meio para a interação e a criação das "bolhas informacionais" (Carvalho, D., 2022).

Nesse sentido, a grande questão a ser discutida é: como as redes sociais moldam a percepção política dos eleitores, uma vez que essa personalização afeta o comportamento e as escolhas políticas. Assim, um dos meios para esse fim é a criação de conteúdos que geram mais engajamento do público, em meio a tantos conteúdos, também surgem as chamadas informações falsas ou, pelo termo popularizado, as fake news, que proporcionam mais comentários e, por terem um maior engajamento, acabam viralizando mais (Carvalho, D., 2022). Conforme assinala Teixeira *et al*. (2018, p. 2) "[...] a evolução da tecnologia contribuiu consideravelmente para o aumento do fluxo de notícias. Com o advento das redes sociais digitais, as informações que, anteriormente, levariam meses para chegar ao outro lado do mundo, hoje chegam em questão de minutos". De acordo com Pedrosa e Baracho Junior (2021, p. 151) "As *fake news* podem prejudicar as eleições na medida em que disseminam notícias que geram desinformação sobre os protagonistas envolvidos no processo eleitoral"

Ademais, a internet tornou-se uma forma barata e muito vantajosa de fazer propaganda política, já que há a possibilidade de alcançar muito mais pessoas do que, por exemplo, pela televisão. Segundo o site de notícias Valor econômico (2020), foi realizado um estudo feito pela UFRJ E FespSP em que 1,2 milhão de tuítes a favor do presidente Jair Bolsonaro eram feitos com a ajuda de software que

identifica robôs, chegando a conclusão de que 55% das publicações pró-Bolsonaro eram feitas por robôs. Nessa direção, esses robôs são os conhecidos bots. Conforme o entendimento do Pedrosa e Baracho Junior (2021, p. 150) a cerca da temática:

> [...] os bots funcionam como influenciadores de votos a partir do momento em que interagem com outros usuários das mídias sociais, debatendo a favor de um candidato e podendo aumentar o número de seguidores ou curtidas de determinado político, gerando a ideia de um apoio inexistente. São projetados para parecer verdadeiros usuários, sendo de difícil distinção para estes.

Dessa forma, a percepção política do eleitor será moldada pelo que ele escolhe consumir, seguida pelo direcionamento de informações com base no mapa de calor do usuário e na maneira como os algoritmos distribuem essas notícias. Sob essa ótica, é possível concluir como a manipulação de dados algorítmicos pode distorcer visões.

## 3.2 MARCO CIVIL DA INTERNET E RESPONSABILIDADE DAS PLATAFORMAS: O QUE A LEGISLAÇÃO BRASILEIRA PREVÊ SOBRE MODERAÇÃO DE CONTEÚDO E DISSEMINAÇÃO DE DESINFORMAÇÃO

O cenário anterior à legislação do Marco Civil da Internet (MCI) era caracterizado por uma forte insegurança jurídica. Tal instabilidade decorria da ausência de regras definidas sobre os deveres de provedores e usuários no que tange a moderação de conteúdo e à atribuição de responsabilidades, resultando em decisões judiciais que variavam a cada caso e afetavam tanto empresas quanto consumidores (Silva, 2024).

Portanto, nessa fase predominou a jurisprudência consolidada pelo STJ, que já se demonstrava alinhada ao pensamento internacional, que estabelecia a aplicação da responsabilidade civil subjetiva aos provedores de aplicações de internet que ignorassem notificações extrajudiciais para remoção de conteúdo (Figueiredo, 2018). Na visão de Silva (2024, p. 55) “toda a estruturação da responsabilidade civil dos provedores de aplicação em relação ao conteúdo gerado por terceiros originou-se da construção jurisprudencial do Superior Tribunal de Justiça sobre o tema”.

Nesse contexto, como resultado direto dessa situação, os debates sobre a necessidade de uma regulamentação abrangente levaram à elaboração do Marco Civil da Internet. No dia 23 de abril de 2014, entrou em vigor o Marco Civil da Internet (MCI), uma legislação que estabelece “princípios, garantias, direitos e deveres para o uso da Internet no Brasil” (Brasil, 2014).

A Lei nº 12.965/2014, conhecida como Marco Civil da Internet ou "Constituição da Internet", estabelece nos seus artigos iniciais os pilares para o ambiente digital, ao mesmo tempo que moderniza e fortalece direitos e garantias já previstos na Constituição Federal de 1988 (Marques; Martins;

Martins, 2024). O que está disposto em conformidade com o pensamento dos autores Marques, Martins e Martins (2024):

> Um dos pilares do MCI, a liberdade de expressão, disposto no art. 2°, é alicerce para outros princípios e garantias da lei. Também disposto no art. 5° e nos arts. 220 ao 224 da Constituição de 1988, bem como no art. 13 do Pacto de São José da Costa Rica, o fundamento reflete a base para uma livre manifestação, comunicação, bem como sobre a liberdade para receber e difundir informações no ambiente digital.

Dessa forma, o foco deve ser a proteção e promoção dos valores constitucionais, para garantir a preservação dos direitos fundamentais e um avanço tecnológico responsável para todos. Pois, a liberdade de expressão é um direito constitucional parte da base para a formação de um Estado Democrático de Direito, em que se faz necessário que os mesmos direitos protegidos fora do ambiente digital sejam, também, garantidos para os usuários da rede online (Faustino, 2020).

A inserção da liberdade de expressão como princípio a ser ponderado nos casos de responsabilidade civil de provedores por conteúdo de terceiros constitui um dos aspectos mais relevantes do seu tratamento no Marco Civil da Internet (Sousa, 2014). A redação do caput do artigo 19 é a seguinte (Brasil, 2014):

> Art. 19. Com o intuito de assegurar a liberdade de expressão e impedir a censura, o provedor de aplicações de internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente, ressalvadas as disposições legais em contrário.

Com base nisso, conforme o Informativo de Jurisprudência n. 823 do Superior Tribunal de Justiça, ficou decidido que "o provedor de aplicação de internet (ex: YouTube) pode, por iniciativa própria, mesmo sem ordem judicial, retirar de sua plataforma conteúdos que violem a lei ou seus termos de uso" (Cavalcante, 2024). Portanto, o REsp n. 2.139.749/SP demonstra que o Superior Tribunal de Justiça considerou legítima a remoção de conteúdo por uma plataforma de vídeo quando há violação de seus termos de uso, enquadrando a moderação como uma atividade lícita de *compliance* interno, não vedada pelo Marco Civil da Internet. Contudo, essa faculdade não é absoluta, pois deve estar subordinada à Constituição e às leis, sujeitando a plataforma à responsabilização por eventuais remoções indevidas (Brasil, 2024). Assim, com o advento do MCI, "o uso dessas plataformas é regulado por termos e condições de serviço e, muitas vezes, está sujeito a moderação para garantir o cumprimento dessas regras" (Silva, 2024, p. 55).

Ademais, com o surgimento da internet a legislação brasileira precisou adotar medidas quanto à disseminação de desinformação no meio digital. De acordo com Souza *et al.* (2024), a disseminação de notícias falsas (fake news) representa um grave risco para as democracias, principalmente quando

envolve períodos eleitorais. Essas informações, criadas intencionalmente para enganar, podem manipular a decisão dos eleitores, prejudicar o debate público e diminuir a confiança geral nas instituições. Segundo entendimento de Souza *et al.* (2024, p.9) "A responsabilização jurídica das plataformas digitais envolve um delicado equilíbrio entre a garantia de uma internet livre, onde a liberdade de expressão seja respeitada, e a necessidade de proteger a integridade do processo eleitoral contra a desinformação". Desse modo, o Marco Civil da Internet surgiu para regulamentar o acesso e a utilização de dados e informações pessoais, tendo como base os princípios constitucionais da liberdade de expressão e da proibição à censura, assegurando assim a livre comunicação e manifestação do pensamento (Almeida *et al.*, 2022). O MCI defende a liberdade de expressão dos usuários, por isso, qualquer remoção de conteúdo online precisa ser feita com muito cuidado para não desrespeitar esse direito.

Além disso, a legislação brasileira, além do MCI, tem avançado visando o combate à desinformação no meio digital. O Projeto de Lei nº 2630/2020 foi proposto com o intuito de combater a desinformação, estabelecendo diretrizes e mecanismos de transparência para redes sociais e serviços de mensagens. O objetivo central é prevenir o uso inadequado dessas plataformas que possam resultar em danos individuais ou coletivos (Souza *et al*., 2024).

Portanto, a Internet possibilita o fortalecimento da participação popular e da democracia no Brasil, já que por meio dela é possível disseminar informações e atingir um vasto número de pessoas. Entretanto, para alcançar esse efeito positivo o amparo legal se mostrou essencial ao atribuir às plataformas responsabilidade quanto à moderação de conteúdo e a disseminação de desinformação.

## 4 CASOS EMBLEMÁTICOS DE COMO A MANIPULAÇÃO DE DADOS PELAS *BIG TECHS* IMPACTA O PROCESSO ELEITORAL

### 4.1 CASO CAMBRIDGE ANALYTICA (EUA, 2016)

O escândalo envolvendo a Cambridge Analytica e o Facebook é um exemplo claro de como a segurança e a privacidade dos usuários são frequentemente negligenciadas. Dessa forma, a consultoria obteve acesso aos dados de milhões de pessoas sem consentimento direto, por meio de um aplicativo que coletava informações não apenas de quem o instalava, mas também de toda a sua rede de amigos, o que representa uma grave falha ética (Schneble; Elger; Shaw, 2018, tradução nossa).

Segundo Oliveira (2021, p.24) "a empresa britânica Cambridge Analytica prestou assessoria na realização de campanhas como a do Brexit e das eleições dos Estados Unidos no ano de 2016". A empresa foi responsável pela campanha do presidente Trump para a presidência dos Estados Unidos, utilizando mineração e análise de dados, bem como métodos para manipular a opinião pública explorando o lado psicológico dos eleitores (Oliveira, 2021). Assim, o escândalo da Cambridge

Analytica teve origem na coleta de dados de 87 milhões de usuários do Facebook por meio do aplicativo *This Is Your Digital Life* (Afriat *et al.,* 2021, tradução nossa).

Nesse contexto, a empresa desenvolveu um modelo preditivo com base em aproximadamente quatro a cinco mil pontos de dados por indivíduo. O objetivo era traçar o perfil de personalidade de cada adulto nos Estados Unidos, partindo do princípio de que a personalidade molda o comportamento e, consequentemente, a decisão de voto. A estratégia consistiu em utilizar esses perfis para direcionar mensagens a eleitores específicos, com a finalidade de influenciar o resultado das eleições norte-americanas de 2016. Constata-se, ainda, que o Facebook tinha conhecimento dessa massiva operação de mineração de dados (Privacidade Hackeada, 2019).

De acordo com o depoimento de Christopher Wylie, cientista de dados da Cambridge Analytica, a empresa empregava aplicativos vinculados ao Facebook para extrair informações não apenas dos usuários diretos, mas também de toda a sua rede de amigos. Assim, esse método permitia acesso irrestrito a dados pessoais, como atualizações de status, *likes* e até mesmo mensagens privadas. Com base nos dados de apenas 270.000 indivíduos, a empresa foi capaz de modelar o perfil psicológico de todo o eleitorado norte-americano (Privacidade Hackeada, 2019). Toda essa operação se trata de uma violação ética, pois manipulou a população de um país durante um processo democrático, sem o conhecimento ou consentimento dos envolvidos.

Além disso, a empresa priorizava eleitores identificados como "os persuasíveis", um grupo com maior probabilidade de ser influenciado. Essa abordagem foi intensificada em estados decisivos, como Michigan, Wisconsin, Pensilvânia e Flórida. Desse modo, para a execução da estratégia, conteúdos customizados eram criados e disseminados em diversas plataformas, como blogs, vídeos e anúncios, visando engajar e, em última instância, manipular a escolha desses eleitores (Privacidade Hackeada, 2019).

Ademais, o caso da Cambridge Analytica impulsionou os legisladores a desenvolverem proteções mais robustas para os dados dos usuários, culminando na ratificação do Regulamento Geral de Proteção de Dados (GDPR) em 2018. Essa regulamentação passou a controlar todas as empresas que lidam com dados de cidadãos da União Europeia, especialmente quando coletam e analisam essas informações de forma sistemática para traçar perfis e prever preferências (Boldyreva; Grishina; Duisembina, 2018, tradução nossa).

O cenário brasileiro também foi influenciado diretamente pelos debates sobre privacidade de dados que se intensificaram com o escândalo da Cambridge Analytica em 2018. O Brasil implementou, em agosto de 2020, a Lei Geral de Proteção de Dados (LGPD) para garantir legalmente a proteção das informações pessoais de seus cidadãos no ambiente digital (Canaan, 2021).

## 4.2 A MODERAÇÃO DE CONTEÚDO NO TELEGRAM E A INTERVENÇÃO DO STF (2022-2023)

De acordo com Monteiro *et al.* (2021), a capacidade de moderação de conteúdo por parte das gigantes da tecnologia é uma fonte de preocupação para múltiplos segmentos, que veem com inquietação a disseminação de desinformação, discursos odiosos e o fomento à violência política. No Brasil, a moderação de conteúdo não era uma preocupação central durante a elaboração do Marco Civil da Internet em 2014. A interpretação predominante da lei é que ela se limita a definir a responsabilidade das plataformas quando não removem conteúdo após uma ordem judicial, o que, por consequência, permite que elas mesmas realizem a moderação de forma proativa.

Em decorrência desses fatos, a moderação nem sempre se torna precisa quanto aos conteúdos publicados, visto que, conforme explica Monteiro *et al.* (2021, p.12), "são cotidianos os episódios de "falsos positivos" e "falsos negativos" no processo de moderação, ou seja, aquele conteúdo que foi excluído mesmo sem violar regra da plataforma e aquele que inequivocamente viola regra e foi mantido, respectivamente"

Nesse sentido, antes de adentrar no caso da moderação de conteúdo no Telegram e a intervenção do STF, é importante ressaltar o que a Lei do Marco Civil da Internet estabelece quanto à requisição de informações dos dados retidos pelas *Big Techs*. Assim, o Supremo Tribunal Federal (2025, p. 6) destaca que :

> A Lei 12.965/2014 estabelece, ainda, em seu art. 11, ser possível a requisição de informações sobre serviços telemáticos diretamente às empresas brasileiras subsidiárias de empresas estrangeiras, quando constituídas sob as leis brasileiras e sediadas no Brasil, pois, nos termos da legislação brasileira, todas as empresas que atuem no território nacional devem estrita obediência ao ordenamento jurídico brasileiro.

Entretanto, esse cenário não foi totalmente concretizado no caso envolvendo o aplicativo de mensagens Telegram. Conforme Silva (2025), a Polícia Federal, em representação ao STF, destacou que o Telegram não apenas é utilizado para atividades ilícitas, mas também construiu uma reputação de não cooperar com as autoridades. Essa postura de desobediência a ordens judiciais e policiais é apresentada pela própria plataforma como um de seus principais atrativos (Dore, 2023).

A plataforma Telegram, mesmo tendo sido criada em 2013 na Rússia e atualmente operando a partir de Dubai, desafiou a soberania jurídica do Brasil ao não cumprir normas e decisões judiciais durante um período eleitoral. Essa postura de desrespeito à legislação foi facilitada pelo fato de a empresa não possuir representação física no território nacional. Desse modo, a disseminação de desinformação foi uma das questões debatidas uma vez que se trata de uma das mais graves interferências causadas por aplicativos de mensagem, cujo design permite grande alcance e entrega automatizada de conteúdo. Essa estrutura facilita a rápida propagação de notícias falsas entre os usuários da rede (Silva, 2025).

No cenário eleitoral de 2022, o pedido de suspensão temporária do Telegram, encaminhado pela Polícia Federal ao STF, ocorreu porque a empresa não respondia a solicitações de informações, incluindo um pedido para remoção de contas de Allan dos Santos e demandas do TSE para combater a disseminação de informações falsas (Carvalho, 2023). De acordo com uma publicação do portal Poder360 (Allan, 2022, online):

> O jornalista bolsonarista Allan dos Santos mantém ativo no Telegram um canal reserva com mais de 22.000 inscritos desde a 6ª feira (25.fev.2022). O perfil foi criado no mesmo dia em que se tornou pública a decisão do ministro Alexandre de Moraes, do Supremo Tribunal Federal, que mandou a plataforma bloquear 3 canais do bolsonarista sob pena de suspensão do aplicativo no país.

Dessa forma, a decisão que determinou o bloqueio do Telegram foi justificada pelo seu descumprimento reiterado de ordens judiciais, pela proliferação de notícias falsas por meio de contas ligadas a Allan dos Santos e pela ocorrência de atos ilícitos em suas comunidades. Essa medida foi tomada após a plataforma atender a uma determinação anterior de forma tardia e incompleta (Dore, 2023).

Ademais, após a suspensão do aplicativo também foi instituído o aumento da multa aplicada de R$100 mil para R$1 milhão por dia em que o Telegram se recusasse a fornecer os dados solicitados pela justiça ( Justiça [...] , 2023)

Com isso, a decisão da primeira instância de bloqueio total do aplicativo foi contrariada em segunda instância, uma vez que o Telegram impetrou mandado de segurança e o bloqueio foi parcialmente suspenso pela 2ª Turma Especializada do TRF2. Segundo o entendimento do desembargador federal Flávio Lucas, a determinação para suspender o Telegram no território nacional era desproporcional, pois prejudicava a comunicação de muitos cidadãos não envolvidos na apuração (Rio de Janeiro, 2023). Assim, o aplicativo foi reativado, mas a multa permaneceu em vigor devido à falha no fornecimento dos dados da investigação (Rio de Janeiro, 2023).

Conclui-se que a ação judicial contra o Telegram no Brasil não é um caso isolado, uma vez que outros países, como Estados Unidos e Alemanha, já haviam aplicado sanções semelhantes por meio de suas Cortes Constitucionais. Esse cenário serve de base para analisar o caso brasileiro sob a ótica da teoria do transconstitucionalismo (Dore, 2023).

## 5 CONSIDERAÇÕES FINAIS

Considerando a crescente influência das *Big Techs* no "jogo de dados" global, como a arquitetura jurídico-constitucional brasileira, no contexto do constitucionalismo multinível, responde aos imperativos de afirmação da soberania digital, especialmente no que tange à capacidade do Estado de regular o tratamento de dados e coibir a manipulação informacional que ameace a autonomia individual e a estabilidade democrática? As análises ao longo do trabalho procuram responder a essa

questão, descrevendo o cenário da soberania digital, o impacto das Big Techs na legislação e sua influência no controle de informações.

Ao descrever o cenário da soberania digital no Brasil, constatou-se que o país, sob um constitucionalismo multinível, adaptou seu ordenamento jurídico aos desafios do meio digital global. A Constituição de 1988 já previa garantias de proteção de dados e privacidade, mas a efetivação da soberania digital exigiu uma evolução legislativa para controlar o fluxo de dados diante da atuação transnacional das Big Techs.

Marcos como o Marco Civil da Internet (MCI) de 2014 e a Lei Geral de Proteção de Dados (LGPD) de 2020 foram passos cruciais para dar segurança jurídica e atribuir responsabilidades às plataformas, equilibrando liberdade de expressão e regulação. Iniciativas como a Política Nacional de Cibersegurança (PNCiber) também demonstram o esforço contínuo do Estado em unificar a regulação e se alinhar às práticas internacionais.

Analisando o impacto das Big Techs, ficou claro que empresas como Google e Meta atuam como gigantes coletoras e processadoras de dados, influenciando comportamentos e discursos. A LGPD, inspirada na GDPR europeu, forçou essas empresas a revisarem suas práticas de coleta e uso de dados, estabelecendo princípios como finalidade, transparência e responsabilização.

A aplicação internacional da LGPD, que alcança operações com dados de brasileiros independentemente da sede da empresa, mostra a intenção do Estado de afirmar sua jurisdição no ambiente digital. No entanto, a complexidade da internet e a falta de uniformidade regulatória global ainda são obstáculos significativos.

Para exemplificar a influência das Big Techs, o estudo detalhou como algoritmos e "bolhas informacionais" moldam a percepção política e podem ser usados para influenciar eleições, inclusive com a disseminação de *fake news* e o uso de bots.

O caso da Cambridge Analytica foi um exemplo notório de manipulação em larga escala, usando dados de usuários do Facebook sem consentimento para influenciar eleições, o que impulsionou legislações de proteção de dados, como a LGPD no Brasil.

No cenário nacional, o caso Telegram demonstrou a tensão entre a soberania do Estado e a falta de cooperação de plataformas transnacionais. A recusa do Telegram em cumprir ordens judiciais sublinhou a urgência de o Brasil reafirmar sua capacidade regulatória para proteger o processo democrático.

Dessa forma, a pesquisa confirma que a arquitetura jurídico-constitucional brasileira tem respondido aos desafios da soberania digital com leis como o MCI e a LGPD, buscando equilibrar liberdade e proteção contra a desinformação. Contudo, o poder transnacional das Big Techs continua sendo um desafio central para a capacidade do Estado de regular efetivamente o fluxo de dados. As

conclusões apontam para a necessidade de adaptação contínua da regulação, por meio de um diálogo multinível, para acompanhar a evolução tecnológica.

Como projeção futura, espera-se que o Brasil fortaleça seus mecanismos de cibersegurança com iniciativas como a PNCiber. A tendência global sugere a criação de leis mais restritivas para empresas que lidam com dados em massa, mas é crucial que essa evolução regulatória não comprometa os direitos fundamentais, evitando que o próprio Estado utilize essas tecnologias de forma abusiva.

## REFERÊNCIAS

55% de publicações pró-Bolsonaro são feitas por robôs. 2020. Valor Econômico. Disponível em: https://valor.globo.com/politica/noticia/2020/04/03/55-de-publicacoes-pro-bolsonaro-sao-feitas-por-robos.ghtml. Acesso em: 18 maio 2025.

AFRIAT, H.; DVIR-GVIRSMAN, S.; TSURIEL, K.; IVAN, L. "This is capitalism. It is not illegal": Users' attitudes toward institutional privacy following the Cambridge Analytica scandal. The Information Society, v. 37, n. 2, p. 115-127, 2021. Disponível em: https://www.tandfonline.com/doi/full/10.1080/01972243.2020.1870596. Acesso em: 09 jul. 2024.

ALLAN dos Santos dribla STF e mantém canal reserva no Telegram. Poder360, 2022. Disponível https://www.poder360.com.br/justica/allan-dos-santos-dribla-stf-e-mantem-canal-reserva-no-telegram. Acesso em: 29 jul. 2025.

ALMEIDA, R. S. de et al. A liberdade de expressão e seus limites: uma análise crítica do marco civil da internet. Research, Society and Development, v. 11, n. 2, e39111225445, 2022. Disponível em: https://rsdjournal.org/index.php/rsd/article/view/25445. Acesso em: 03 jul. 2025.

ALMEIDA, S. N. de C.; COSTA, F. A. V. A. Segurança x privacidade: entendendo a nova lei geral de proteção de dados pessoais nº 13.709/2018. Revista de Direito & Desenvolvimento da UniCatólica, [S. l.], v. 6, n. 1, p. 56–70, 2023. Disponível em: http://publicacoes.unicatolicaquixada.edu.br/index.php/rdd/article/view/444. Acesso em: 3 maio. 2025.

BATTISTI, Roberta. Regulação das Big Techs. São Paulo: Almedina Brasil, 2023.

BOLDYREVA, E. L.; GRISHINA, N. Y.; DUISEMBINA, Y. Cambridge Analytica: ethics and online manipulation with decision-making process. The European Proceedings of Social & Behavioural Sciences, v. 12, p. 92-102, dez. 2018. DOI: 10.15405/epsbs.2018.12.02.10. Acesso em: 9 jul. 2025.

BRASIL. [Constituição da República Federativa do Brsil de 1988]. Constituição da República Federativa do Brasil de 1988. Brasília, DF: Presidência da República, Casa Civil, Subchefia para Assuntos Jurídicos. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 17 maio 2025.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Disponível em: www.planalto.gov.br. Acesso em: 17 maio 2025a.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais. Brasília, DF: Presidência da República, Casa Civil, Subchefia para Assuntos Jurídicos. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 17 de maio.

BRASIL. Gabinete de Segurança Institucional da Presidência da República. PNCiber – Apresentação do Projeto. 2023. Acesso em: 05 maio 2025.

BRASIL. Superior Tribunal de Justiça. Informativo de Jurisprudência n. 823. Brasília, DF, 10 de junho de 2024. Disponível em: https://processo.stj.jus.br/jurisprudencia/externo/informativo/?acao=pesquisarumaedicao&livre=0823.cod.&from=feed. Acesso em: 2 jul. 2025.

BRASIL. Supremo Tribunal Federal. Despacho (PET 9.935/DF). Relator: Min. Alexandre de Moraes. Brasília, DF, 19 fev. 2025b. Disponível em:https://www.migalhas.com.br/arquivos/2025/2/83CF55DB926D19_pet9935rumble.pdf. Acesso em: 29 jul. 2025.

CANAAN, Renan Gadoni. Estímulo à inovação através de regulamentações para a proteção de dados pessoais: o impacto da replicação da GDPR na LGPD. Ottawa: Centre for Law, Technology and Society, University of Ottawa, [2021?].

CARVALHO, Ana Caroline Melo. Desinformação, democracia e internet: o bloqueio de plataformas e a relação política nas eleições de 2022. 2023. Disponível em : https://repositorio.ufersa.edu.br/server/api/core/bitstreams/739eaaca-6493-4066-ad08-069ea2524d26/content. Acesso em 28 jul. 2025.

CARVALHO, Douglas Belchior de. As big techs e a moderação de conteúdo eleitoral. 2022. Disponível em: https://dspace.mackenzie.br/items/f2331cbb-fcfd-4390-93a9-1a609e00acb0Acesso em: 25 abr. 2025.

CARVALHO, Lucas Borges de. Soberania digital: legitimidade e eficácia da aplicação da lei na internet. Revista Brasileira de Direito, Passo Fundo, v. 14, n. 2, p. 213-235, maio/ago. 2018.

CAVALCANTE, Márcio André Lopes. O provedor de aplicação de internet (ex: YouTube) pode, por iniciativa própria, mesmo sem ordem judicial, retirar de sua plataforma conteúdos que violem a lei ou seus termos de uso. 2024 Disponível em: https://www.buscadordizerodireito.com.br/jurisprudencia/detalhes/6fb993285d56e6927284ff9b11ac6851. Acesso em: 03 jul. 2025

CAVALLARO, Amanda de Castro. O impacto do monopólio das big techs na privacidade e proteção de dados pessoais. 2021. Disponível em: https://repositorio.ufpb.br/jspui/handle/123456789/28553. Acesso em 25 abr. 2025

CONSTITUCIONALISMO MULTINIVE. LTA Sul. [ S. I.: s.n.], 2019. 1 vídeo (4:12 min). Tradução: Google tradutor. Disponível em: https://wG1ww.youtube.com/watch?v=7gdL9Hmqh0U. Acesso em: 17 mar. 2025.

DORE, B. G. Análise da decisão do supremo tribunal federal que determinou a suspensão do telegram: um novo precedente de transconstitucionalismo no brasil?. Revista Contemporânea, [S. l.], v. 3, n. 8, p. 13008–1330, 2023. DOI: 10.56083/RCV3N8-168. Disponível em: https://ojs.revistacontemporanea.com/ojs/index.php/home/article/view/1539. Acesso em: 02 de jul. 2025.

FAUSTINO, André. Fake news: a liberdade de expressão nas redes sociais na sociedade da informação. São Caetano do Sul/SP: Lura Editorial, 2020. Disponível em: https://books.google.com.br/books.com. Acesso em: 13 maio 2025

FIGUEIREDO, Ana Luiza Canuto de. Responsabilidade civil dos provedores de aplicação de internet: crítica às inovações trazidas pelo Marco Civil da Internet. Rio de Janeiro: Universidade Federal do Rio de Janeiro, 2018. Disponível em: https://pantheon.ufrj.br/bitstream/11422/6144/1/ALCFigueiredo.pdf. Acesso em: 02 de jul. 2025

JUSTIÇA determina suspensão do Telegram no Brasil. Infomoney. Abr. de 2023. Disponível em : https://www.infomoney.com.br/consumo/justica-determina-suspensao-do-telegram-no-brasil/. Acesso em : 29 de jul. 2025

LEY, Isabelle. Proteção Jurídica Contra o Conselho de Segurança da ONU: Entre o Direito Europeu e o Direito Internacional: Uma Situação Kafkiana?: Relatório sobre a conferência de outono do programa de pós-graduação "Constitucionalismo Multinível (Verfassung jenseits des Staates)", em Berlim, 8 de dezembro de 2006. Revista Alemã de Direito , v. 8, n. 3, p. 279-293, 2007. Acesso em 24 abr. 2025

MARQUES, Claudia Lima; MARTINS, Guilherme Magalhães; MARTINS, Fernando Rodrigues. 10 anos marco civil da internet: Avaliando impactos e desafios. Cotia: Foco, 2024. E-book. Disponível em: https://plataforma.bvirtual.com.br. Acesso em: 01 jun. 2025.

MEGAVAZAMENTO de dados de 223 milhões de brasileiros: o que se sabe e o que falta saber. G1, 28 jan. 2021. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/2021/01/28/vazamento-de-dados-de-223-milhoes-de-brasileiros-o-que-se-sabe-e-o-que-falta-saber.ghtml\. Acesso em: 13 maio 2025.

MONTEIRO, Artur Pericles Lima; CRUZ, Francisco Brito; SILVEIRA, Juliana Fonteles da; VALENTE, Mariana G. Armadilhas e caminhos na regulação da moderação de conteúdo. Diagnósticos & Recomendações. São Paulo: InternetLab, 2021.

OLIVEIRA, Caio José Arruda Amarante de; MOREIRA, Thiago Oliveira. El Constitucionalismo Multinivel Interamericano y el diálogo (necesario) entre el Supremo Tribunal Federal de Brasil y la Corte Interamericana de Derechos Humanos en materia de prisión preventiva. ESTUDIOS CONSTITUCIONALES, v. 21, n. 1, 2023. DOI: 10.4067/S0718-52002023000100279.

OLIVEIRA, Letícia Costa. O uso de dados pessoais na era digital como forma de manipulação social e ameaça à democracia: um estudo de caso da Cambridge Analytica. 2021. 63 f. Trabalho de Conclusão de Curso (Graduação em Relações Internacionais) - Escola de Direito e Relações Internacionais, Pontifícia Universidade Católica de Goiás, Goiânia, 2021.

PEDROSA, Clara Bonaparte; BARACHO JUNIOR, José Alfredo de Oliveira. Algoritmos, bolha informacional e mídias sociais: desafios para as eleições na era da sociedade da informação. Revista Thesis Juris – RTJ, São Paulo, v. 10, n. 1, p. 148-164, jan./jun. 2021. Disponível em: doi.org. Acesso em: 18 maio 2025.

PELIZZARI, Bruno Henrique Miniuchi; BARRETO JUNIOR, Irineu Francisco. Bolhas sociais e seus efeitos na sociedade da informação: ditadura do algoritmo e entropia na internet. Revista de Direito, Governança e Novas Tecnologias, Belém, v. 5, n. 2, p. 57-73, jul./dez. 2019.

PEREIRA, Luana Mendes. A regulação das Big Techs no Brasil e sua responsabilidade pelo combate ao discurso de ódio: perspectivas e desafios.Bahia, 2024.Disponível em: https://saberaberto.uneb.br/items/8bfc975a-90c4-46ee-bb96-56c46cfa4656. Acesso em: 29 jul. 2025.

PÉREZ CONCHILLO, Eloísa. El derecho de acceso a la información pública en el marco del constitucionalismo multinivel y de la actual crisis sanitaria. Revista de Derecho Político, [S. l.], n. 109, p. 229-260, set.-dez. 2020.

PRIVACIDADE HACKEADA. Direção: Karim Amer e Jehane Noujaim. Europa: Netflix, 2019.

REGULAÇÃO de Big Techs no Direito Digital: Desafios e Soluções. Legale Educacional Blog, [S.l.], 6 jun. 2024. Disponível em:https://encurtador.com.br/UCDw

RIO DE JANEIRO. Tribunal regional federal DA 2ª REGIÃO. TRF2 cassou em parte liminar que suspendeu provisoriamente funcionamento do Telegram no Brasil. Rio de Janeiro, 29 abr. 2023. Disponível em:www.trf2.jus.br. Acesso em: 29 jul. 2025.

SANCTIS JÚNIOR, Rubens José Kirk de. A REGULAÇÃO DAS BIG TECHS NO BRASIL: UM IMPERATIVO DEMOCRÁTICO. Revista da Seção Judiciária do Rio de Janeiro, [S.l.], v. 28, n. 60, p. 74-100, mar. 2024. ISSN 2177-8337. Disponível em:http://lexcult.trf2.jus.br/index.php/revistasjrj/article/view/793. Acesso em: 25 abr. 2025.

SCHNEBLE, C. O.; ELGER, B. S.; SHAW, D. The Cambridge Analytica affair and Internet-mediated research. EMBO reports, v. 19, n. e46579, jul. 2018. DOI: 10.15252/embr.201846579. Disponível em: www.embopress.org. Acesso em: 09 jul. 2025.

SILVA, Iris Nathalia da. Liberdade de Expressão e Responsabilidade Civil nas Plataformas de Redes Sociais: As Insuficiências do Marco Civil da Internet. 2024. 110 f. Trabalho de Conclusão de Curso (Graduação em Direito) – Centro de Ciências Jurídicas, Universidade Federal de Santa Catarina, Florianópolis, 2024.

SILVA, Lucas Lima. Tensões entre as Big techs e o Estado brasileiro: uma análise sobre o descumprimento de decisões judiciais pelo Telegram e pelo X/Twitter e sobre a interferência no processo legislativo pelo Google. 2025. Monografia (Graduação em Direito) – Câmpus Universitário de Arraias, Universidade Federal do Tocantins, Arraias, 2025.

SOARES, R. R. Lei Geral de Proteção de Dados – LGPD: direito à privacidade no mundo globalizado. 2020. 31 f. Monografia Jurídica (Trabalho de Conclusão de Curso) - Pontifícia Universidade Católica de Goiás, Goiânia, 2020.

SOUSA, Carlos Affonso Pereira de. As cinco faces da proteção à liberdade de expressão no Marco Civil da Internet. Rio de Janeiro, 2014. Disponível em https://share.google/bOBg6lv7vOQakyiJX. Acesso em: 09 jul. 2025.

SOUZA, Alcian Pereira de et al. Impacto das fake news no processo eleitoral e a responsabilidade jurídica das plataformas digitais. Revista Contribuciones a Las Ciencias Sociales, São José dos Pinhais, v.17, n.10, p. 01-14, 2024. DOI: 10.55905/revconv.17n.10-133.

TEIXEIRA, Vitoria Matheus et al. As fake news e suas consequências nocivas à sociedade. Itaperuna, RJ: Universidade Iguaçu, [2018?]. 11 p.

UNIÃO EUROPEIA. Disposições gerais. 2018. Disponível em: https://gdpr-info.eu/chapter-1/. Acesso em: 24 abr. 2025.

UNIÃO EUROPEIA. Capítulo 3. Direitos do titular dos dados. In: GDPR Info. [S.l.: s.n.], 2018. Disponível em: gdpr-info.eu. Acesso em: 3 maio 2025.