VIII ENCONTRO VIRTUAL DO CONPEDI

INTERNET: DINÂMICAS DA SEGURANÇA PÚBLICA E INTERNACIONAL

I61

Internet: dinâmicas da segurança pública internacional [Recurso eletrônico on-line] organização CONPEDI

Coordenadores: Irineu Francisco Barreto Junior; José Carlos Francisco dos Santos; Yuri Nathan da Costa Lannes. – Florianópolis: CONPEDI, 2025.

Inclui bibliografia
ISBN: 978-65-5274-137-0
Modo de acesso: www.conpedi.org.br em publicações
Tema: Direito Governança e Políticas de Inclusão

1. Direito – Estudo e ensino (Pós-graduação) – Encontros Nacionais. 2. Internet. 3. Segurança pública internacional. VIII Encontro Virtual do CONPEDI (2; 2025; Florianópolis, Brasil).

CDU: 34

Conselho Nacional de Pesquisa
e Pós-Graduação em Direito Florianópolis
Santa Catarina – Brasil
www.conpedi.org.br

VIII ENCONTRO VIRTUAL DO CONPEDI

INTERNET: DINÂMICAS DA SEGURANÇA PÚBLICA E INTERNACIONAL

Apresentação

O VIII Encontro Virtual do CONPEDI, organizado pelo CONPEDI, teve como tema central "Direito Governança e Políticas de Inclusão". A partir dessa temática, foram promovidos intensos debates entre pesquisadores nacionais e internacionais, com apresentações de trabalhos previamente selecionados por meio de avaliação duplo-cega por pares.

Os artigos reunidos nesta publicação foram apresentados no Grupo de Trabalho "Internet: Dinâmicas da segurança pública e internacional", realizado no dia 25 de junho de 2025, e refletem o estado atual das pesquisas desenvolvidas por graduandos e pós-graduandos em direito em diversas instituições brasileiras. O conjunto de trabalhos revela a diversidade temática e a profundidade das discussões jurídicas contemporâneas sobre os impactos da tecnologia na sociedade.

As apresentações cobriram uma ampla gama de tópicos que envolvem a interface entre tecnologia, direito, internet, segurança pública e segurança internacional, demonstrando um panorama das preocupações acadêmicas sobre privacidade, desinformação e desigualdades digitais. Com o intuito de facilitar a leitura e destacar os enfoques abordados, os trabalhos foram organizados nos seguintes eixos temáticos:

1. Inteligência Artificial, Cidades Inteligentes e Tomada de Decisão - Este eixo reúne estudos que tratam dos desafios e vulnerabilidades da adoção da inteligência artificial, especialmente nas cidades inteligentes, e discute os efeitos da automação sobre os processos decisórios e o papel do Direito na sua regulação:

Uma Reflexão sobre a Proteção de Dados e o Direito Brasileiro (Flávio Bento, Marcia Hiromi Cavalcanti)

O Direito ao Esquecimento e sua Aplicação nos Tribunais Brasileiros (Davi Niemann Ottoni, Matheus Oliveira Maia, Claudiomiar Vieira Cardoso)

3. Crimes Digitais, Segurança Pública e Cooperação Internacional - Este eixo aborda os novos contornos da criminalidade digital, como crimes virtuais e lavagem de dinheiro online, analisando as respostas do sistema jurídico, as políticas públicas e a necessidade de cooperação internacional:

Políticas Públicas e o Enfrentamento de Crimes Virtuais (Bruno Augusto Alves Tuma, Anna Verena Alves Tuma)

O Crime de Lavagem de Dinheiro Digital: Uma Análise sob as Perspectivas da Segurança Pública, os Desafios da Legislação Brasileira e a Importância da Cooperação Internacional (Francislene Aparecida Teixeira Morais)

4. Desinformação, Mídia e Processo Eleitoral - Nesta seção, os autores analisam os impactos das novas dinâmicas midiáticas, da comunicação em redes sociais e da desinformação no processo eleitoral brasileiro, propondo reflexões jurídicas sobre liberdade de expressão e regulação da informação.

Os Princípios Constitucionais da Comunicação Social no Brasil e os Desafios da Era Digital à Luz das Novas Dinâmicas Midiáticas (Andreia Ponciano de Moraes Joffily, Fabrício Meira Macêdo)

Os Desafios Jurídicos e Impactos da Desinformação no Processo Eleitoral Brasileiro

Espera-se que esta publicação contribua para o aprofundamento dos debates sobre os desafios jurídicos da era digital, estimulando novas reflexões e a produção científica crítica e inovadora. Agradecemos a todos os pesquisadores, pareceristas e organizadores que tornaram este Grupo de Trabalho possível. Desejamos uma excelente leitura!

Irineu Francisco Barreto Junior - FMU

José Carlos Francisco dos Santos - Faculdades Londrina

Yuri Nathan da Costa Lannes - FDF

UMA REFLEXÃO SOBRE A PROTEÇÃO DE DADOS E O DIREITO BRASILEIRO

A REFLECTION ON DATA PROTECTION AND BRAZILIAN LAW

Flávio Bento [1]
Marcia Hiromi Cavalcanti [2]

Resumo

Este artigo propõe uma análise aprofundada sobre a proteção de dados pessoais no contexto da sociedade tecnológica brasileira, tendo como foco as questões e desafios em busca de valores democráticos de justiça e igualdade para as relações humanas em sociedade, diante do cenário contemporâneo, destacando a influência do Poder Judiciário na salvaguarda dos direitos constitucionais. A partir da Constituição Federal de 1988, do Marco Civil da Internet [Lei nº 12.965/2014], da Lei Geral de Proteção de Dados [Lei nº 13.709/2018], e da jurisprudência do Supremo Tribunal Federal, investiga-se a tensão entre inovação tecnológica e direitos fundamentais. O estudo enfatiza o papel do STF na consolidação do direito à proteção de dados, a importância da governança ética, e os mecanismos de compliance como instrumentos normativos em prol da democracia e da dignidade da pessoa humana. Defende-se um comportamento ético e moral das empresas, por meio da adoção de instrumentos de autorregulação. Ao estabelecer parâmetros normativos sólidos, incentivar a transparência e a prestação de contas, as empresas podem contribuir para a prevenção da utilização inadequada dos dados, bem como para a contenção do poder exercido pelas grandes empresas de tecnologia, alinhado aos princípios fundamentais, para prevenir e conter a financeirização dos dados e o poder das Big Techs.

Palavras-chave: Proteção de dados, Estado democrático de direito, Big techs, Compliance, Direitos fundamentais

Abstract/Resumen/Résumé

This article proposes an in-depth analysis of personal data protection in the context of the Brazilian technological society, focusing on the issues and challenges in the search for

innovation and fundamental rights is investigated. The study emphasizes the role of the STF in consolidating the right to data protection, the importance of ethical governance, and compliance mechanisms as normative instruments in favor of democracy and human dignity. Ethical and moral behavior of companies is defended, through the adoption of self-regulatory instruments. By establishing solid regulatory parameters, encouraging transparency and accountability, companies can contribute to preventing the inappropriate use of data, as well as containing the power exercised by large technology companies, in line with fundamental principles, to prevent and contain the financialization of data and the power of Big Techs.

Keywords/Palabras-claves/Mots-clés: Data protection, Democratic rule of law, Big techs, Compliance, Fundamental rights

1. INTRODUÇÃO

A revolução digital transformou radicalmente as estruturas sociais, políticas e econômicas, inaugurando um novo regime de produção, circulação e apropriação de informações.

Nesse contexto, a proteção de dados emerge como direito fundamental cuja efetividade depende da articulação entre ordenamento jurídico, instituições estatais e sociedade civil. Daí a importância de se estudar a segurança das informações pessoais, que estão em risco diante dessa realidade atual.

No Brasil, a Constituição de 1988, em conjunto com a Lei Geral de Proteção de Dados Pessoais [LGPD], representa um marco estruturante na defesa da privacidade e da autodeterminação informacional, pontos centrais das reflexões expressas neste estudo.

Este trabalho tem como objetivo principal examinar a influência do Poder Judiciário, especialmente do Supremo Tribunal Federal [STF], na consolidação normativa e jurisprudencial da proteção de dados, analisando decisões relevantes, a atuação da Autoridade Nacional de Proteção de Dados [ANPD] e os desafios contemporâneos da regulação digital.

A pesquisa adota a modalidade teórica, centrada na análise e na reflexão quanto à necessidade de compreensão de conceitos, de ideias, de teorias, objetivando aprofundar os conhecimentos teóricos sobre o tema e a problematização propostas. A técnica de pesquisa é essencialmente a bibliográfica e a documental.

2. FUNDAMENTOS CONSTITUCIONAIS E O DIREITO À PROTEÇÃO DE DADOS

A Constituição da República Federativa do Brasil de 1988 estabelece, em seu artigo 5º, incisos X e XII, os pilares fundamentais da proteção à intimidade, à vida privada, à honra e à imagem das pessoas, bem como ao sigilo das comunicações. A Constituição também assegura o direito ao acesso à informação [inciso XIV], compondo um conjunto normativo que baliza a tutela da privacidade no ordenamento jurídico pátrio.

A consagração do direito à proteção de dados como direito fundamental foi reforçada pela decisão do Supremo Tribunal Federal na ADI 6387, em 2020, que reconheceu a autonomia desse direito em relação à privacidade, estabelecendo-o como elemento central à dignidade da pessoa humana. Nessa decisão, o STF apontou que a coleta, o tratamento e o uso de dados pessoais devem estar submetidos ao controle do titular e à fiscalização por autoridades independentes.

A proteção de dados também se insere no rol de garantias constitucionais implícitas decorrentes do princípio da dignidade da pessoa humana [art. 1º, III], do direito à igualdade [art. 5º, caput], da liberdade [art. 5º, II] e da inviolabilidade da intimidade. O reconhecimento da autodeterminação informativa — expressão da liberdade individual sobre o uso de suas informações pessoais — decorre dessa leitura constitucional ampliada.

E o princípio da dignidade da pessoa humana orienta todo o Direito brasileiro como um direito fundamental, porque coloca a pessoa no "centro das atenções", o que é fundamental na sociedade moderna e dominada pela tecnologia, pelas grandes empresas digitais. Conforme leciona Paulo Nalin, não há espaço para os "valores egoísticos" do Direito tradicional, mas sim os valores coletivos:

> Ocorre que resgatar o homem (antropocentrismo) não se identifica com a renovação daqueles valores egoísticos contidos no Código Civil, ou seja, não é o homem econômico que figura no vértice constitucional, em que pese ser este também tutelado pela Carta, todavia de forma casual, mas sim, o homem existencial, recepcionada a relação jurídica desde que tais experiências individuais tenham uma projeção útil (existencial) para o titular em si e para o coletivo. (2008, p. 244)

Além disso, o artigo 3º da Carta Magna, ao prever como objetivos fundamentais da República a construção de uma sociedade livre, justa e solidária, bem como a erradicação da pobreza e a redução das desigualdades sociais e regionais, exige que o Estado promova políticas públicas que garantam o acesso democrático à informação, sem que isso implique em violação à privacidade.

Portanto, a proteção de dados, além de encontrar respaldo direto nos dispositivos constitucionais, é elemento estruturante de uma sociedade democrática de direito. A sua efetividade depende da atuação harmônica entre os Poderes da República, especialmente do Poder Judiciário, que tem desempenhado papel de vanguarda na delimitação dos contornos desse novo direito fundamental no Brasil.

3. A SOCIEDADE VIGIADA

A sociedade contemporânea está inserida em um contexto de transformação digital acelerada, no qual os dados pessoais se tornaram um dos ativos mais valiosos para o mercado. A digitalização das relações sociais e a popularização da *internet* promoveram uma nova lógica econômica pautada na coleta massiva, armazenamento e tratamento de dados — fenômeno que a autora Shoshana Zuboff denominou "capitalismo de vigilância" (2020).

E mesmo que a sociedade considere o conforto, a agilidade e a segurança das tratativas *on-line* de certa forma libertadoras, em um paradoxo, seus dados e comportamento são capturados e se tornam um mercado de comportamento, um produto de alto valor. Esta também é a leitura que Habermas faz das sociedades modernas e a colonização do mundo da vida:

> as sociedades modernas capitalistas são marcadas cada vez mais, segundo Habermas, por fenômenos novos de violência, reificação e alienação que não resultam diretamente de estruturas de classe. Os próprios conflitos de classe são relativamente apaziguados por uma série de fatores. Entre eles, conta-se primeiramente a intervenção estatal na economia, seja para manter ou aumentar as taxas de crescimento, seja para evitar ou absorver crises econômicas. Além disso, a participação no sistema político é generalizada por meio das democracias de massas, de modo que a dominação política se legitima na maior parte da população. Ao mesmo tempo, os conflitos sociais são institucionalizados juridicamente, isto é, estabelecem-se legislações sobre relações de trabalho e seguridade social. Também o sistema educacional se expande, possibilitando maiores margens de mobilidade social. O conceito que Habermas forja para compreender esse processo todo é o conceito de colonização sistêmica do mundo da vida. Ou seja, os sistemas dinheiro e poder se comportam como senhores coloniais que invadem de fora uma sociedade tribal, usurpam seus recursos naturais e forçam os nativos a assimilar as regras do senhor. Em suma, o sistema invade e coloniza o mundo da vida (NOBRE, 2018).

Essa nova economia de dados estabelece um regime de controle informacional, em que as atividades humanas, desde as mais banais até as mais íntimas, são monitoradas, quantificadas e convertidas em produtos comercializáveis. Grandes empresas de tecnologia, as chamadas Big Techs, operam sob essa lógica e, muitas vezes, à margem ou à frente da legislação vigente, tornando-se verdadeiros entes transnacionais com poder político e econômico comparável ao de Estados soberanos.

Hoje, as maiores empresas do mundo, à frente das grandes financeiras e das petrolíferas, são a Apple, o Google e a Microsoft, que dominam as plataformas digitais. São empresas transnacionais com o capital avaliado maior que o PIB de muitos países. O Estado muitas vezes não tem como efetivar direitos frente a esse mercado, e mesmo as garantias fundamentais como a dignidade, a igualdade e a segurança jurídica não podem ser asseguradas. Mesmo casos mais simples, como uma compra online em uma empresa no exterior, fogem ao controle do Estado. O usuário de redes digitais é dragado por centenas de milhares de informações que são selecionadas e filtradas em equações algorítmicas. A capacidade de discernimento da pessoa é subjugada pela inteligência artificial. O que passa um sentimento de segurança e conforto pode estar ameaçando os direitos mais básicos do cidadão, no mundo da pós-verdade, onde a verdade é relativa ou não interessa ao indivíduo. A

pessoa se torna um produto frente a essa dominação do mundo da vida, e surge a necessidade de buscar na teoria crítica alguma segurança.

No Brasil, a penetração dessas plataformas digitais ocorre em meio a uma realidade socioeconômica marcada por desigualdades estruturais, o que potencializa os riscos à privacidade e à autodeterminação informacional dos indivíduos. Milhões de brasileiros, ao utilizarem serviços gratuitos em redes sociais, mecanismos de busca e aplicativos, acabam cedendo seus dados sem plena consciência ou controle sobre os usos que deles serão feitos.

A captura de dados em larga escala, muitas vezes realizada sem o consentimento informado do titular, constitui grave ameaça aos direitos fundamentais. Não se trata apenas de uma questão de privacidade, mas de liberdade, dignidade e justiça social. Como apontam Frazão e Carvalho (2022), os dados pessoais têm dupla natureza: são, ao mesmo tempo, projeções da personalidade e recursos econômicos que devem ser protegidos por uma lógica jurídica e ética.

O Poder Judiciário brasileiro, ciente desse cenário, tem sido chamado a intervir em diversas demandas que envolvem a relação entre consumidores e plataformas digitais, vazamentos de dados, uso de inteligência artificial e decisões automatizadas. Tais conflitos revelam a urgência de uma regulação efetiva, pautada por princípios constitucionais, que assegure os direitos dos cidadãos frente ao avanço do capitalismo de vigilância.

Dessa forma, é necessário compreender que a proteção de dados, em uma sociedade tecnológica, vai além de uma agenda de privacidade. Trata-se de uma questão de soberania informacional, que exige do Estado brasileiro, especialmente do Judiciário, respostas firmes e estruturadas para conter os abusos do poder informacional e garantir a prevalência dos direitos constitucionais sobre interesses econômicos hegemônicos.

4. A LGPD COMO MARCO NORMATIVO BRASILEIRO

A promulgação da Lei nº 13.709/2018, conhecida como Lei Geral de Proteção de Dados Pessoais [LGPD], representou um divisor de águas no ordenamento jurídico brasileiro ao estabelecer um regime jurídico específico para o tratamento de dados pessoais, inspirado no Regulamento Geral de Proteção de Dados [GDPR] da União Europeia.

A LGPD se estrutura em torno de princípios fundamentais como a finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização. Tais princípios visam garantir que o

tratamento de dados seja realizado de forma ética, segura e proporcional aos direitos fundamentais do titular.

A lei define o tratamento de dados pessoais como toda operação realizada com dados, como a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração. Essa definição amplia o espectro de situações que devem ser reguladas pelo diploma legal.

A relação da economia e da sociedade com a captura de dados está em constante interação, repercutindo sobre as liberdades individuais e a própria democracia.

O fenômeno, longe de se restringir à seara econômica, apresenta inúmeras repercussões nas esferas individuais dos cidadãos, além de levar à total reestruturação das relações sociais e políticas. Consequentemente, os dados ganharam uma importância transversal, tornando-se elementos centrais para a compreensão das vidas e das liberdades individuais, assim como da sociedade e da própria democracia. Uma economia movida a dados está, portanto, intrinsecamente relacionada a uma sociedade movida a dados e também a uma política movida a dados, sendo que todas essas esferas se encontram em constante interação (FRAZÃO, CARVALHO, 2022).

O ordenamento brasileiro, como tantos outros, vem sendo construído. A Lei n° 12.965/2014 (BRASIL, 2014), o chamado Marco Civil da Internet, pretendeu regular o uso da Internet no Brasil pela previsão de princípios, garantias, direitos e deveres para quem usa a rede, e de diretrizes para a atuação do Estado. Em 2018 veio a Lei Geral de Proteção de Dados Pessoais, a Lei de nº 13.709 (BRASIL, 2018), para regular o tratamento de dados pessoais e alterou os artigos 7º e 16 do Marco Civil da Internet. No mesmo ano foi promulgada na União Europeia Regulamento Geral sobre a Proteção de Dados [GDPR], e o *California Consumer Privacy Act of 2018* [CCPA], nos Estados Unidos da América, todas com a instrumentalização semelhante ao *Compliance*, chamado de instrumento de conformidade, que no Brasil está previsto na Lei nº 12.846/2013 (BRASIL, 2013), a Lei Anticorrupção, alicerçada nos pilares da governança, da transparência, da prestação de contas, da equidade e da responsabilidade corporativa.

Os dados capturados representam um capital ativo para o mercado e para a política.

> [...] dados tanto se apresentam como relevante ativo social, político e econômico, a ser inclusive quantificado quando da avaliação do patrimônio das companhias, quanto constituem verdadeiros desdobramentos da personalidade dos indivíduos e, por conseguinte, merecem relevante

> proteção sob a esfera existencial (FRAZÃO, CARVALHO e MARTINEZ, 2022).

A Lei Geral de Proteção de Dados brasileira tem por objetivo assegurar patamares mínimos e obrigatórios de proteção dos dados pessoais a todos aqueles que estejam sujeitos à sua incidência.

A razão de ser da proteção da privacidade e dos dados pessoais não é propriamente o resguardo do sigilo ou da intimidade, mas sim impedir que agentes de tratamento usem o imenso poder que decorre dos dados contra os seus titulares. Daí por que a tutela de dados pessoais não diz respeito propriamente a esconder aspectos privados das vidas dos indivíduos, mas sim a estabelecer o controle das informações a seu respeito e delimitar o poder que os agentes de tratamentos têm a partir dessas informações, inclusive para o fim de impedir que exerçam tal poder contra a população (FRAZÃO, 2022).

A LGPD também cria direitos específicos aos titulares de dados, como o direito à confirmação da existência de tratamento, ao acesso aos dados, à correção de dados incompletos, à anonimização, bloqueio ou eliminação de dados desnecessários, e à portabilidade dos dados, entre outros. Esses direitos refletem a autodeterminação informativa e visam reforçar o poder do indivíduo frente aos agentes de tratamento.

No plano institucional, a LGPD previu a criação da Autoridade Nacional de Proteção de Dados [ANPD], com a função de zelar, implementar e fiscalizar o cumprimento da lei em todo o território nacional. A ANPD é responsável por editar normas, aplicar sanções, promover estudos e fomentar boas práticas no setor público e privado.

No contexto jurídico-constitucional, a LGPD reforça a proteção da dignidade da pessoa humana, da liberdade e da privacidade, concretizando direitos fundamentais previstos na Constituição Federal. A lei também impõe deveres de *compliance* às empresas e ao poder público, exigindo a implementação de políticas internas, relatórios de impacto à proteção de dados e medidas de segurança da informação.

Quanto ao *compliance*, destaque-se que ele precisa ir além de uma mera estratégia de gestão da organização, e deve estabelecer uma cultura que valoriza o cumprimento de todas as obrigações legais e éticas, promovendo assim a responsabilidade e o respeito aos direitos fundamentais. A LGPD se assemelha em muitos aspectos ao programa de integridade, pautado na Lei n. 12.846 de 2013, que promove uma cultura de conformidade, orientada pelo cumprimento das normas e das leis e pela integridade, buscando fazer o que é correto, moral e ético. Para a prevenção das hipóteses legais, as instituições são orientadas para a gestão de

riscos, o controle e a transparência no uso e armazenamento de dados, o que pode satisfazer os interesses do Estado, da sociedade e da empresa.

A aplicação da LGPD pelo Judiciário tem evidenciado a importância do equilíbrio entre inovação tecnológica e respeito aos direitos fundamentais. Casos de vazamento de dados, decisões automatizadas e tratamento ilícito de informações têm sido analisados sob a ótica dos princípios constitucionais e da LGPD, demonstrando a crescente judicialização do tema e a necessidade de interpretação conforme a Constituição. Assim, a LGPD representa não apenas uma resposta normativa às exigências contemporâneas da sociedade digital, mas também um instrumento de realização dos valores constitucionais da democracia, cidadania, igualdade e justiça social

5. A ATUAÇÃO DO STF NA PROTEÇÃO DE DIREITOS DIGITAIS

O Supremo Tribunal Federal [STF], como guardião da Constituição Federal de 1988, tem desempenhado papel central na conformação do direito à proteção de dados pessoais como um direito fundamental, bem como na regulamentação do uso ético e democrático da tecnologia da informação no Brasil.

A atuação da Corte pode ser observada em decisões paradigmáticas que reafirmam o vínculo entre privacidade, liberdade e dignidade da pessoa humana. Um dos casos emblemáticos é a Ação Direta de Inconstitucionalidade [ADI] 6387[1], na qual o STF declarou

[1] MEDIDA CAUTELAR EM AÇÃO DIRETA DE INCONSTITUCIONALIDADE. REFERENDO. MEDIDA PROVISÓRIA Nº 954/2020. EMERGÊNCIA DE SAÚDE PÚBLICA DE IMPORTÂNCIA INTERNACIONAL DECORRENTE DO NOVO CORONAVÍRUS (COVID-19). COMPARTILHAMENTO DE DADOS DOS USUÁRIOS DO SERVIÇO TELEFÔNICO FIXO COMUTADO E DO SERVIÇO MÓVEL PESSOAL, PELAS EMPRESAS PRESTADORAS, COM O INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA. FUMUS BONI JURIS. PERICULUM IN MORA. DEFERIMENTO. 1. 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. 2. Na medida em que relacionados à identificação – efetiva ou potencial – de pessoa natural, o tratamento e a manipulação de dados pessoais hão de observar os limites delineados pelo 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), sob pena de lesão a esses direitos. O compartilhamento, com ente público, de dados pessoais custodiados por concessionária de serviço público há de assegurar mecanismos de proteção e segurança desses dados. 3. O Regulamento Sanitário Internacional (RSI 2005) adotado no âmbito da Organização Mundial de Saúde exige, quando essencial o tratamento de dados pessoais para a avaliação e o manejo de um risco para a saúde pública, a garantia de que os dados pessoais manipulados sejam "adequados, relevantes e não excessivos em relação a esse propósito" e "conservados apenas pelo tempo necessário." (artigo 45, § 2º, alíneas "b" e "d"). 4. Consideradas a necessidade, a adequação e a proporcionalidade da medida, não emerge da Medida Provisória nº 954/2020, nos moldes em que editada, interesse público legítimo no compartilhamento dos dados pessoais dos usuários dos serviços de telefonia. 5. Ao não definir apropriadamente como e para que serão utilizados os dados coletados, a MP nº 954/2020 desatende a garantia do devido processo legal (art. 5º, LIV, da CF), na dimensão substantiva, por não oferecer condições de avaliação quanto à sua adequação e necessidade, assim entendidas como a compatibilidade do tratamento com as

a inconstitucionalidade de dispositivos da Medida Provisória nº 954/2020 que autorizava o compartilhamento de dados de usuários de telecomunicações com o IBGE durante a pandemia da COVID-19, sem consentimento explícito e sem garantias adequadas de segurança e finalidade. O julgamento consolidou o entendimento de que a proteção de dados pessoais é direito fundamental autônomo, exigindo estrita observância aos princípios constitucionais.

Outro exemplo relevante é o Inquérito 4781[2], conhecido como o inquérito das *fake news*, em que o STF reafirmou a necessidade de responsabilidade das plataformas digitais e da proteção da integridade da informação como valor essencial à democracia. Nesse caso, o

---

finalidades informadas e sua limitação ao mínimo necessário para alcançar suas finalidades. 6. Ao não apresentar mecanismo técnico ou administrativo apto a proteger, de acessos não autorizados, vazamentos acidentais ou utilização indevida, seja na transmissão, seja no tratamento, o sigilo, a higidez e, quando o caso, o anonimato dos dados pessoais compartilhados, a MP nº 954/2020 descumpre as exigências que exsurgem do texto constitucional no tocante à efetiva proteção dos direitos fundamentais dos brasileiros. 7. Mostra-se excessiva a conservação de dados pessoais coletados, pelo ente público, por trinta dias após a decretação do fim da situação de emergência de saúde pública, tempo manifestamente excedente ao estritamente necessário para o atendimento da sua finalidade declarada. 8. Agrava a ausência de garantias de tratamento adequado e seguro dos dados compartilhados a circunstância de que, embora aprovada, ainda não vigora 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. O fragilizado ambiente protetivo impõe cuidadoso escrutínio sobre medidas como a implementada na MP nº 954/2020. 9. O cenário de urgência decorrente da crise sanitária deflagrada pela pandemia global da COVID-19 e a necessidade de formulação de políticas públicas que demandam dados específicos para o desenho dos diversos quadros de enfrentamento não podem ser invocadas como pretextos para justificar investidas visando ao enfraquecimento de direitos e atropelo de garantias fundamentais consagradas na Constituição. 10. Fumus boni juris e periculum in mora demonstrados. Deferimento da medida cautelar para suspender a eficácia da Medida Provisória nº 954/2020, 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. 11. Medida cautelar referendada.

[2] Ementa: PENAL E PROCESSUAL PENAL. FORTES INDÍCIOS DE PARTICIPAÇÃO DO INVESTIGADO EM ORGANIZAÇÃO CRIMINOSA ("MILÍCIAS DIGITAIS").UTILIZAÇÃO DE PERFIS NAS REDES SOCIAIS PARA A PROPAGAÇÃO DE DISCURSOS COM CONTEÚDO DE ÓDIO, SUBVERSÃO DA ORDEM E INCENTIVO À QUEBRA DA NORMALIDADE INSTITUCIONAL E DEMOCRÁTICA. ABUSO DO DIREITO DE LIBERDADE DE EXPRESSÃO. NECESSIDADE E ADEQUAÇÃO NO BLOQUEIO DE PERFIL PARA FAZER CESSAR A ATIVIDADE CRIMINOSA. AGRAVO REGIMENTAL A QUE SE NEGA PROVIMENTO. 1. O objeto deste inquérito é a investigação de notícias fraudulentas (fake news), falsas comunicações de crimes, denunciações caluniosas, ameaças e demais infrações revestidas de animus caluniandi, diffamandi ou injuriandi, que atingem a honorabilidade e a segurança do SUPREMO TRIBUNAL FEDERAL, de seus membros; bem como de seus familiares, quando houver relação com a dignidade dos Ministros, inclusive o vazamento de informações e documentos sigilosos, com o intuito de atribuir e/ou insinuar a prática de atos ilícitos por membros da SUPREMA CORTE por parte daqueles que têm o dever legal de preservar o sigilo; e a verificação da existência de esquemas de financiamento e divulgação em massa nas redes sociais, com o intuito de lesar ou expor a perigo de lesão a independência do Poder Judiciário e o Estado de Direito. 2. As diligências iniciais, descritas nos autos, especialmente na decisão datada de 26/5/2020, indicam a existência de uso organizado de ferramentas de informática, notadamente contas em redes sociais, para criar, divulgar e disseminar informações falsas ou aptas a lesar as instituições do Estado de Direito, notadamente o SUPREMO TRIBUNAL FEDERAL. 3. Necessidade, adequação e urgência na interrupção dos discursos com conteúdo de ódio, subversão da ordem e incentivo à quebra da normalidade institucional e democrática mediante bloqueio de contas em redes sociais, tais como Facebook, Twitter e Instagram, dos investigados, com objetivo de interromper a lesão ou ameaça a direito (art. 5º, XXXV, Constituição Federal). 4. Os investigados apontados teriam, em tese, ligação direta ou indireta com a associação criminosa e seu financiamento, pois, avaliando-se o teor de seus pronunciamentos e procedimento de divulgação em redes sociais, notam-se indícios de alinhamento de suas mensagens ilícitas com o suposto esquema narrado pelos parlamentares ouvidos nestes autos. 5. Agravo Regimental desprovido. (Inq 4781 AgR-nono, Relator(a): ALEXANDRE DE MORAES, Tribunal Pleno, julgado em 03-07-2023, ACÓRDÃO ELETRÔNICO DJe-s/n DIVULG 08-09-2023 PUBLIC 11-09-2023)

tribunal tem atuado contra a disseminação sistemática de desinformação e discursos de ódio, utilizando prerrogativas constitucionais para proteger o Estado Democrático de Direito.

A jurisprudência do STF tem se mostrado sensível à necessidade de controle sobre algoritmos e decisões automatizadas, à luz dos direitos à transparência, ao contraditório e à ampla defesa. A Corte reconhece que o uso intensivo de tecnologia pelo poder público e por empresas privadas não pode violar garantias constitucionais, sob pena de desvirtuamento da própria ordem jurídica democrática.

A atuação do STF evidencia, assim, um esforço contínuo de concretização de um novo patamar de proteção dos direitos fundamentais, adequado às exigências da era digital. Tal protagonismo revela o papel crucial do Poder Judiciário na regulação do espaço informacional e na contenção dos riscos sistêmicos representados pelo poder das *Big Techs* e pelo uso indiscriminado de dados pessoais.

A interferência do STF tem sido fundamental não apenas para reconhecer a proteção de dados como um direito constitucional, mas também para estabelecer parâmetros normativos e axiológicos que orientem a conduta dos agentes públicos e privados na sociedade da informação.

6. O COMBATE À DESINFORMAÇÃO E A RESPONSABILIDADE DAS PLATAFORMAS

O fenômeno da desinformação se tornou uma das mais graves ameaças à integridade das democracias contemporâneas. Alimentada pelo uso indiscriminado de tecnologias digitais, por redes de disseminação de *fake news* e pela manipulação algorítmica de conteúdos, a desinformação impacta diretamente o direito à informação, à liberdade de expressão e à participação política consciente e plural.

No Brasil, a gravidade do problema levou à atuação direta do Supremo Tribunal Federal, como observado no Inquérito 4781 e nas ações correlatas ao combate às *fake news*. A Corte tem reiterado a necessidade de responsabilização das plataformas digitais por omissão no controle de conteúdo ilícitos, inclusive quando esses atentam contra a ordem democrática, os direitos fundamentais e a segurança institucional.

A jurisprudência brasileira caminha para reconhecer que as plataformas, ao oferecerem espaços públicos digitais, tornam-se corresponsáveis pela mediação da informação. Esse entendimento decorre do princípio da função social da comunicação e da

vedação ao abuso do direito à liberdade de expressão, que não se confunde com a permissão de propagação de mentiras com potencial lesivo à democracia.

O Marco Civil da Internet [Lei nº 12.965/2014], embora estabeleça diretrizes importantes sobre a neutralidade de rede e a privacidade, demanda atualização legislativa para enfrentar os novos contornos da desinformação algorítmica. Nesse sentido, propostas legislativas como o Projeto de Lei das *Fake News* [PL 2630/2020] buscam regulamentar a atividade das plataformas e exigir transparência algorítmica, rastreabilidade de conteúdos e deveres de diligência em casos de violação de direitos.

Independentemente de posições ou conclusões sobre essa questão das *fake news*, Evgeny Morozov observa que:

> o problema não são as fake news, e sim a velocidade e a facilidade de sua disseminação, e isso acontece principalmente porque o capitalismo digital de hoje faz com que seja alativas falsas que atraem cliques (2018, 184).

No ambiente das plataformas sociais e das mídias, a utilização das *fake news* são uma concreta ameaça aos direitos humanos e à democracia. Assim como a utilização inadequada e ilegal dos dados, a utilização das *fake news*, em todas as suas possibilidades, especialmente na Política, se tornou um instrumento de agressividade, desrespeito, sem qualquer atenção aos interesses públicos e aos princípios constitucionais.

Além da via legislativa, o Poder Judiciário tem adotado medidas cautelares para remoção de conteúdos falsos, bloqueio de contas e responsabilização civil e penal dos agentes propagadores de desinformação. Tais medidas visam proteger o debate público qualificado e preservar o processo democrático, especialmente em períodos eleitorais.

A responsabilização das plataformas não é incompatível com a liberdade de expressão. Ao contrário, trata-se de assegurar um ambiente informacional saudável, livre de manipulação, que respeite os direitos fundamentais e promova o pluralismo. A atuação do STF e de outras instâncias judiciais aponta para um novo paradigma normativo: o da regulação democrática do espaço digital, com protagonismo institucional e participação cidadã.

7. A CULTURA E A GOVERNANÇA ÉTICA

É essencial consolidar uma cultura institucional voltada à ética, à responsabilidade e à transparência. A LGPD traz um conjunto de medidas organizacionais destinadas a assegurar o

tratamento adequado das informações pessoais, mitigando riscos e promovendo a integridade institucional.

Tais práticas não se limitam à obediência normativa. Elas demandam uma mudança cultural no setor público e privado, com a adoção de códigos de conduta, canais de denúncia, treinamentos permanentes e auditorias regulares. O compromisso ético se torna elemento central da governança moderna e instrumento de construção de confiança entre os entes econômicos, o Estado e os cidadãos.

Além da atuação do Estado, uma opção importante é a elaboração de instrumentos e códigos privados pelas empresas, como o *compliance*. Nesse sentido, a perspectiva normativa da governança ou da administração da *internet* é aceita como "um conjunto de instrumentos normativos que engloba, dentre outros, tratados internacionais, regulações governamentais e instrumentos de direito privado e códigos e diretrizes caracterizados com soft law" (KELLER, 2019, p. 267).

A governança ética exige, ainda, que as organizações se comprometam com os direitos dos titulares de dados e com os princípios constitucionais que regem o ordenamento jurídico brasileiro. A efetividade dessa conduta, está diretamente relacionada à adesão voluntária aos valores democráticos e à capacidade de prevenir violações antes que elas ocorram.

Ao pensar em uma "governança democrática de conteúdo online", na diversificação dos mecanismos de coordenação e de controle das plataformas, seja sob a perspectiva pública, de políticas pública, como no enfoque da atuação das organizações empresariais e de sua visão de responsabilidade social, é possível trabalhar na superação das limitações da regulação atual, marcada pela "remoção de conteúdo" e na responsabilização por danos.

Nesse cenário, o Poder Judiciário também atua como indutor de boas práticas, exigindo a demonstração de boa-fé, responsabilidade e diligência por parte dos agentes econômicos e entidades públicas. O STF já reconheceu que a ausência de mecanismos de prevenção de proteção de dados, pode configurar omissão relevante na proteção dos direitos fundamentais.

8. A AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD) E O CONTROLE ADMINISTRATIVO

A Autoridade Nacional de Proteção de Dados [ANPD] é um órgão essencial à estrutura normativa da LGPD. Sua função reguladora, fiscalizadora e orientadora a posiciona como protagonista na implementação da política nacional de proteção de dados. A ANPD tem

como atribuições editar diretrizes, fiscalizar práticas, aplicar sanções e fomentar a cultura da proteção de dados. Sua atuação deve ser independente, técnica e fundamentada nos direitos e garantias fundamentais previstos na Constituição Federal.

A criação da ANPD também permitiu o avanço do controle administrativo sobre o setor privado e o poder público, estabelecendo padrões de transparência, prestação de contas e segurança da informação. A existência da autoridade fortalece o sistema de freios e contrapesos e potencializa a eficácia social da LGPD.

9. DESAFIOS PARA A EFETIVAÇÃO DOS DIREITOS DIGITAIS NO BRASIL

Apesar dos avanços normativos, diversos desafios persistem para a efetivação dos direitos digitais no Brasil. A cultura de vigilância, a precariedade da educação digital, as desigualdades no acesso à informação e a resistência de setores econômicos ao cumprimento da LGPD são entraves à consolidação da proteção de dados como valor democrático.

A baixa estruturação técnica de muitas organizações, inclusive no setor público, compromete a implementação plena das exigências legais. Além disso, a insuficiência de recursos e a fragilidade institucional da ANPD ainda limitam sua capacidade de fiscalização e sanção.

Outro desafio importante diz respeito à ausência de uma legislação mais robusta sobre o uso ético de algoritmos e inteligência artificial. A ausência de normas específicas pode levar à violação sistemática de direitos fundamentais, em especial o direito à igualdade e à não discriminação.

Espera-se que a interação das partes, bem como a atualização e o fortalecimento dos marcos regulatórios, contribua para a construção de um ambiente mais ético, transparente e responsável na utilização dos dados, reduzindo os riscos de violações dos direitos fundamentais e promovendo a segurança jurídica e uma sociedade mais justa e equitativa. É claro que qualquer prognóstico depende das ações e das medidas adotadas pela sociedade, empresas e instituições governamentais, assim como a certificação das medidas implementadas.

CONSIDERAÇÕES FINAIS

A proteção de dados pessoais constitui uma das principais agendas jurídicas do século XXI. No Brasil, os marcos constitucionais, legais e jurisprudenciais apontam para uma consolidação do direito à autodeterminação informativa como pilar da cidadania digital.

O Poder Judiciário brasileiro, e em especial o Supremo Tribunal Federal, tem desempenhado papel fundamental na defesa dos direitos constitucionais frente aos desafios impostos pelas tecnologias digitais. O reconhecimento do direito à proteção de dados como direito fundamental e a responsabilização das plataformas por desinformação e abuso informacional revelam o compromisso institucional com a democracia, a liberdade e a dignidade.

A articulação entre LGPD, atuação judicial, ANPD e políticas de compliance configura um ecossistema normativo que, embora ainda em construção, revela grande potencial para assegurar os direitos fundamentais no ambiente digital.

É possível também promover um comportamento ético e moral das empresas, por meio da adoção de instrumentos de autorregulação. Ao estabelecer parâmetros normativos sólidos, incentivar a transparência e a prestação de contas, as empresas podem contribuir para a prevenção da utilização inadequada dos dados, bem como para a contenção do poder exercido pelas grandes empresas de tecnologia, alinhado aos princípios fundamentais, para prevenir e conter a financeirização dos dados e o poder das *Big Techs*.

O fortalecimento da cultura jurídica da proteção de dados exige o engajamento contínuo de todos os atores sociais: legisladores, magistrados, administradores públicos, empresas e cidadãos. Somente por meio dessa aliança será possível construir um espaço informacional justo, plural e democrático.

REFERÊNCIAS BIBLIOGRÁFICAS

BARROSO, Luís Roberto. **Curso de Direito Constitucional Contemporâneo - Os conceitos Fundamentais**. eBook Kindle: Saraiva, 2022.

BOBBIO, N**. O futuro da democracia: uma defesa das regras do jogo.** Trad. Marco Aurélio Nogueira. Rio de Janeiro: Paz e Terra, 1986.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 18 abr. 2025.

BRASIL. **Lei n. 12.965, de 23 de abril de 2014**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 18 abr. 2025.

BRASIL. **Lei n. 13.709, de 14 de agosto de 2018**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 18 abr. 2025.

BRASIL. **Lei n. 12.846, de 1 de agosto de 2013**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12846.htm. Acesso em: 16 abr. 2025.

DOWBOR, Ladislau (Org.). **Sociedade Vigiada: Como a Invasão da Privacidade, por Grandes Corporações e Estados Autoritários, Ameaça Instalar uma Nova Distopia** por Vicente Argentino Netto Valdir Ap. Mafra. São Paulo: Autonomia Literária, 2020.

FRAZÃO AZEVEDO LOPES, Ana. Inteligência Artificial e Direito: Ética, Regulação e Responsabilidade. Rio de Janeiro: Revista dos Tribunais, 2019.

FRAZÃO AZEVEDO LOPES; Ana SALOMÃO; Luis Felipe; VILLAS BÔAS CUEVA. **Lei de Liberdade Econômica e seus impactos no direito brasileiro.** eBook Kindle. Rio de Janeiro: Thomson Reuters, Revista dos Tribunais, 2019.

FRAZÃO AZEVEDO LOPES; CARVALHO, Angelo Prata de, MILANEZ, Giovanna. **Curso de Proteção de Dados - Fundamentos da LGPD** eBook Kindle, Forense, 2022.

FRAZÃO AZEVEDO LOPES; CARVALHO, Angelo Prata de. **Lei de Liberdade Econômica: Análise Crítica**. eBook Kindle, Forense, 2022.

GIDDENS, Anthony e SUTTON, Philip W. **Conceitos essenciais da Sociologia**. 2 ed. Tradução Claudia Freire. São Paulo: UNESP, 2017.

GIDDENS, Anthony; LASH, Scott; BECK, Ulrich: **Modernização reflexiva**. São Paulo: UNESP, 1995.

HABERMAS, Jürgen. **Direito e democracia. Entre facticidade e validade,** São Paulo: Tempo Brasileiro, 1997.

KELLER, Clara Iglesias. **Regulação nacional de serviços na internet: exceção, legitimidade e o papel do Estado**. 2019. Tese. (Doutorado em Direito). Universidade do Estado do Rio de Janeiro, Faculdade de Direito. 2019.

NALIN, Paulo. **Do contrato, conceito pós-moderno. Em busca de sua Formação na perspectiva civil-constitucional**. 2 ed. Curitiba: Editora Juruá, 2008.

NOBRE, Marcos. **Curso livre de Teoria Crítica**. Campinas: Papirus, 2018. eBook Kindle.

MOROZOV, Evgeny. **BIG TECH, A ascensão dos dados e a morte da política.** Tradução Cláudio Marcondes. São Paulo: Ubu, 2018.

SAAD, Elizabeth. **Sociedade digitalizada: "plataformarização" das relações e uma privacidade "zerada".** São Paulo, Jornal da USP, 2019. Disponível em: https://jornal.usp.br/artigos/sociedade-digitalizada-plataformizacao-das-relacoes-e-uma-privacidade-zerada/. Acesso em: 15 abr. 2025.

SATHLER, André Rehbein, FERREIRA, Renato Soares Peres. **Declaração Universal dos Direitos Humanos Comentada** eBook Kindle, Brasília, DF: Edições Câmara, 2022.

ZUBOFF, Shoshana. **The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power**: Barack Obama's Books of 2019, E.Book Kindle, London: Profile Books, 2019.

ZUBOFF, Shoshana. **A era do capitalismo de vigilância: a luta por um futuro humano na nova fronteira de poder**. Tradução de George Schlesinger. Rio de Janeiro: Intrínseca, 2020.