ARTIGO

A PROTEÇÃO DE DADOS PESSOAIS NO BRASIL: AVANÇOS NORMATIVOS E DESAFIOS PRÁTICOS NA APLICAÇÃO DA LGPD

PERSONAL DATA PROTECTION IN BRAZIL: REGULATORY ADVANCES AND PRACTICAL CHALLENGES IN THE APPLICATION OF LGPD

Sandra Analia dos Santos[1]
Bacharel em Direito - UniCuritiba
Especialista em Ética e Direitos Humanos - Fapad
Especializanda em Compliance na Gestão Pública - Faculdade Estácio
Agente de Controle Interno - Fundepar

RESUMO

A proteção de dados pessoais assume centralidade no ordenamento jurídico brasileiro contemporâneo, sendo reconhecida pela Emenda Constitucional n.º 115/2022 como direito fundamental autônomo, integrante do rol do art. 5º da Constituição da República Federativa do Brasil de 1988. Essa conquista normativa é fruto de um processo histórico que, embora iniciado com instrumentos esparsos de tutela da intimidade, consolidou-se com o advento do Marco Civil da Internet (Lei n.º 12.965/2014) e da Lei Geral de Proteção de Dados Pessoais – LGPD (Lei n.º 13.709/2018, alterada pela Lei n.º 13.853/2019). A LGPD, inspirada no Regulamento Geral de Proteção de Dados da União Europeia (GDPR), estabelece princípios como finalidade, necessidade, transparência e segurança, exigindo do Estado e das particulares condutas proativas de salvaguarda. Entretanto, a mera positivação normativa não tem sido suficiente para conter os recorrentes vazamentos de dados, que comprometem não apenas a privacidade individual, mas também a credibilidade institucional e a estabilidade democrática. Casos emblemáticos — como a exposição massiva de milhões de brasileiros em fóruns clandestinos entre 2021 e 2023, o ataque hacker ao sistema da CEDAE no Rio de Janeiro, e o escândalo Cambridge Analytica no cenário internacional — demonstram que a proteção de dados enfrenta entraves de ordem técnica, cultural e política. Soma-se a isso a deficiência estrutural da Autoridade Nacional de Proteção de Dados (ANPD), ainda carente de autonomia, recursos e efetividade sancionatória, além da postura por

1 Contato: sandrasas@fundepar.pr.gov.br

vezes leniente do Poder Judiciário. O presente artigo tem por objetivo analisar criticamente os avanços normativos e os desafios práticos da aplicação da LGPD, expondo desde seus fundamentos constitucionais até a atuação jurisprudencial do STF e do STJ. Busca-se demonstrar que a proteção de dados transcende o campo normativo: trata-se de imperativo ético, político e social, vinculado à própria noção de dignidade da pessoa humana e essencial à consolidação da democracia digital.

PALAVRAS-CHAVE

LGPD. Dados pessoais. Dignidade da pessoa humana. Vazamentos de dados. Jurisprudência.

ABSTRACT

The protection of personal data assumes centrality in the contemporary Brazilian legal system, being recognized by Constitutional Amendment No. 115/2022 as an autonomous fundamental right, part of the list of art. 5th of the Constitution of the Federative Republic of Brazil of 1988. This normative achievement is the result of a historical process that, although started with sparse instruments for the protection of privacy, was consolidated with the advent of the Marco Civil da Internet (Law no. 13,853/2019). The LGPD, inspired by the European Union's General Data Protection Regulation (GDPR), establishes principles such as purpose, necessity, transparency and security, requiring proactive safeguarding conduct from the State and individuals. However, mere normative affirmation has not been enough to contain recurrent data leaks, which compromise not only individual privacy, but also institutional credibility and democratic stability. Emblematic cases — such as the massive exposure of millions of Brazilians in clandestine forums between 2021 and 2023, the hacker attack on the CEDAE system in Rio de Janeiro, and the Cambridge Analytica scandal on the international scene — demonstrate that data protection faces technical, cultural and political obstacles. Added to this is the structural deficiency of the National Data Protection Authority (ANPD), which still lacks autonomy, resources and sanctioning effectiveness, in addition to the sometimes lenient stance of the Judiciary. This article aims to critically analyze the normative advances and practical challenges of applying the LGPD, exposing its constitutional foundations to the jurisprudential performance of the STF and the STJ. The aim is to demonstrate that data protection transcends the normative field: it is an ethical, political and social imperative, linked to the very notion of human dignity and essential to the consolidation of digital democracy.

KEYWORDS

LGPD. Personal data. Human dignity. Data breaches. Jurisprudence.

ARTIGO

1 INTRODUÇÃO

A sociedade contemporânea vive sob a égide da informação. Se, em épocas pretéritas, a propriedade da terra, o domínio dos meios de produção ou o capital financeiro constituíam os principais vetores de poder, hoje, no século XXI, é inegável que os dados pessoais assumiram esse papel estratégico. Informações aparentemente banais — como nome, CPF, endereço eletrônico, hábitos de consumo, preferências culturais ou convicções políticas — passaram a ter valor econômico inestimável, transformando-se em mercadorias que circulam em mercados formais e, sobretudo, informais, muitas vezes sem o conhecimento ou consentimento de seus titulares.

Esse novo cenário impôs ao Direito a necessidade de repensar categorias tradicionais e de criar instrumentos normativos aptos a salvaguardar a dignidade da pessoa humana em sua dimensão informacional. A Constituição da República Federativa do Brasil de 1988, em sintonia com a tradição garantista inaugurada no pós-guerra, já havia estabelecido no art. 5º, incisos X e XII, a inviolabilidade da intimidade, da vida privada e do sigilo das comunicações. Mais recentemente, a Emenda Constitucional n.º 115/2022 elevou a proteção de dados pessoais ao patamar de direito fundamental autônomo**,** inserindo-o explicitamente no rol das cláusulas pétreas. Trata-se de marco histórico, pois confere densidade normativa à ideia de que a privacidade não se resume à esfera doméstica ou íntima, mas se estende ao controle que cada indivíduo deve exercer sobre as informações que lhe dizem respeito — a chamada autodeterminação informativa**.**

Contudo, até a consolidação desse direito, o Brasil percorreu trajetória complexa. Antes mesmo da positivação constitucional expressa, diversos diplomas normativos buscaram oferecer proteção fragmentada, a exemplo do Código Civil e do Código Penal. No entanto, apenas com o Marco Civil da Internet (Lei n.º 12.965/2014) o país passou a dispor de uma legislação de caráter geral voltada à regulação do ambiente digital, visando princípios como neutralidade da rede, privacidade e liberdade de expressão. Embora significativo, o Marco Civil revelou-se insuficiente para tratar de forma abrangente do ciclo de vida dos dados pessoais — coleta, tratamento, armazenamento e compartilhamento.

Foi nesse contexto que surgiu a Lei Geral de Proteção de Dados Pessoais (LGPD – Lei n.º 13.709/2018, alterada pela Lei n.º 13.853/2019)**,** claramente inspirada no Regulamento Geral de Proteção de Dados da União Europeia (GDPR). A LGPD estabeleceu princípios, direitos e deveres aplicáveis a todos os agentes de tratamento de dados, sejam eles públicos ou privados, impondo critérios de transparência, finalidade e proporcionalidade. Além disso, criou a Autoridade Nacional de Proteção de Dados (ANPD)**,** órgão encarregado de fiscalizar, regulamentar e sancionar condutas em desconformidade com a legislação.

Apesar de tais avanços, a experiência prática revela que a mera existência de legislação não basta para conter as ameaças concretas. Vazamentos de dados em larga escala — alguns acidentais, outros dolosamente praticados por organizações criminosas — continuam a ocorrer, expondo cidadãos a fraudes, discriminações e manipulações políticas. Casos como o da Cambridge Analytica**,** que utilizou informações de milhões de usuários do Facebook para interferir em processos eleitorais, e, no Brasil, a exposição de dados de milhões de consumidores e cidadãos em fóruns clandestinos, demonstram que a proteção de dados é não apenas questão de privacidade, mas também de segurança nacional e estabilidade democrática**.**

A problemática se agrava diante de dois fatores adicionais: (i) a fragilidade institucional da ANPD**,** cuja autonomia é limitada e cuja estrutura técnica ainda se mostra insuficiente; e (ii) a postura leniente do Poder Judiciário, que por vezes relativiza a gravidade dos vazamentos, deixando de impor sanções efetivamente dissuasórias. Some-se a isso a carência de cultura de proteção de dados no seio da sociedade brasileira, em que prevalece uma certa banalização da privacidade, como se a exposição de informações fosse mero efeito colateral do mundo digital.

Assim, a presente pesquisa tem por objetivo analisar criticamente os avanços normativos e os desafios práticos da aplicação da LGPD no Brasil, percorrendo seus fundamentos constitucionais, os episódios emblemáticos de vazamentos, as dificuldades de atuação da ANPD e a forma como o Poder Judiciário tem enfrentado a matéria.

Parte-se da premissa de que a proteção de dados pessoais não se esgota no cumprimento formal de dispositivos legais: trata-se de um imperativo ético, político e social**,** que visa resguardar a dignidade da pessoa humana e assegurar a efetividade da cidadania em tempos de democracia digital. Proteger dados pessoais é, em última instância, proteger o próprio ser humano e o espaço democrático em que se insere.

2 FUNDAMENTOS CONSTITUCIONAIS E AVANÇOS NORMATIVOS

A proteção de dados pessoais não emerge de modo isolado no ordenamento jurídico brasileiro. Ao contrário, insere-se em um processo evolutivo que encontra raízes no princípio da dignidade da pessoa humana (art. 1º, III, da Constituição Federal), verdadeiro vetor axiológico que irradia para todo o sistema normativo. A dignidade humana, compreendida como núcleo dos direitos fundamentais, exige que cada indivíduo seja reconhecido como sujeito autônomo, capaz de decidir sobre sua vida privada e, por extensão, sobre as informações que lhe dizem respeito.

Nesse sentido, a Constituição de 1988 já consagrava, em seu art. 5º, incisos X e XII, a inviolabilidade da intimidade, da vida privada, da honra, da imagem e do sigilo das comunicações. Tais dispositivos, embora relevantes, foram concebidos em um

contexto anterior à massificação da internet e à economia de dados. Assim, embora assegurassem proteção à esfera íntima e ao sigilo, mostraram-se insuficientes diante das novas formas de coleta e tratamento informacional que caracterizam a era digital.

O avanço mais expressivo se deu com a Emenda Constitucional n.º 115/2022, que inseriu expressamente no art. 5º, inciso LXXIX, o direito fundamental à proteção de dados pessoais, inclusive nos meios digitais**.** A alteração não se limita a um aspecto formal: ela projeta a proteção de dados como direito autônomo, desvinculado de outras garantias da personalidade, e coloca o Brasil em sintonia com a tendência internacional de reconhecer a autodeterminação informativa como direito fundamental.

Sob a perspectiva infraconstitucional, dois diplomas assumem relevância central: o Marco Civil da Internet (Lei n.º 12.965/2014) e a Lei Geral de Proteção de Dados Pessoais (Lei n.º 13.709/2018)**.**

O Marco Civil da Internet, por muitos considerado a "Constituição da Internet", estabeleceu princípios como a neutralidade de rede, a liberdade de expressão e a proteção da privacidade. Contudo, sua abordagem ainda era ampla e insuficiente para disciplinar de forma detalhada o ciclo de tratamento de dados pessoais.

A lacuna foi preenchida com a edição da LGPD, que, inspirada no Regulamento Geral sobre a Proteção de Dados da União Europeia (GDPR)**,** instituiu um regime normativo completo e específico para o tratamento de dados pessoais por pessoas físicas e jurídicas, de direito público ou privado. A lei definiu conceitos centrais (art. 5º), estabeleceu princípios de aplicação obrigatória (art. 6º) e disciplinou os direitos dos titulares, bem como as obrigações dos controladores e operadores.

Os princípios da LGPD constituem seu núcleo axiológico:

a) finalidade**,** impondo que o tratamento de dados se dê para propósitos legítimos, específicos e informados ao titular;

b) necessidade, vedando a coleta excessiva;

c) Adequação**,** exigindo compatibilidade entre a finalidade e o tratamento realizado;

d) transparência, garantindo clareza nas práticas adotadas;

e) segurança**,** obrigando a adoção de medidas técnicas e administrativas para proteger os dados;

f) responsabilização e prestação de contas, impondo ao agente o dever de demonstrar conformidade.

Por último, mas de realce até na lei, desponta a boa-fé, no caput, com os seguintes itens *infojobs*: "As atividades de tratamento de dados pessoais deverão observar a

boa-fé, determinando que o indivíduo e os dados pessoais componham parceria no sentido de que inexistirão vícios e ilegalidades arquitetados intencionalmente".

No plano institucional, a LGPD criou a Autoridade Nacional de Proteção de Dados (ANPD), concebida como órgão responsável por regulamentar, fiscalizar e aplicar sanções administrativas. Todavia, apesar de sua importância, a ANPD enfrenta críticas quanto à sua autonomia funcional e financeira, pois sua vinculação inicial à Presidência da República limitou sua independência decisória, além da escassez de recursos humanos e tecnológicos para enfrentar o crescente número de incidentes de segurança.

No direito comparado, nota-se que a LGPD seguiu de perto a experiência europeia. O GDPR, aprovado em 2016 e em vigor desde 2018, consolidou a proteção de dados como um direito fundamental na União Europeia, estabelecendo regras rígidas para transferência internacional de dados e impondo sanções significativas às empresas infratoras. A LGPD, embora guiada nesse modelo, apresenta divergências notáveis: a ausência inicial de autonomia plena da ANPD e a limitação das multas aplicáveis no Brasil enfraquecem seu potencial dissuasório, o que explica, em parte, a continuidade dos vazamentos em larga escala.

Dessa forma, pode-se afirmar que os avanços normativos brasileiros são inegáveis, especialmente após a constitucionalização expressa do direito à proteção de dados. Contudo, esses avanços ainda não se traduziram em proteção eficaz. Entre a norma e a realidade permanece um hiato, sustentado por entraves culturais, tecnológicos e institucionais, que será explorado nas seções seguintes deste estudo.

ARTIGO

3 VAZAMENTOS DE DADOS PESSOAIS: FATOS E EXEMPLOS EMBLEMÁTICOS

3.1 ACESSO

Em legislação de amplitude e rigor que tem por objetivo produzir texto que, efetivamente, impeça o vazamento indiscriminado de dados pessoais em posse do Poder Público, parece paradoxal a constatação das múltiplas possibilidades de acesso aos dados pessoais, como, por exemplo, em um capítulo inteiro da lei (Lei n. 12.527/2011, o cap. II, arts 6°, 7°, 8° e 9°), e também outras orientações no capítulo III, com os Procedimentos de Acesso à Informação;

Tanto maior pode parecer a estranheza e o paradoxo ao se ler:

> Cabe aos órgãos e entidades do poder público, observadas as normas e procedimentos específicos aplicáveis, assegurar a:
> I - gestão transparente da informação propiciando amplo acesso a ela e sua divulgação [1]

1 Lei 12. 527 de 2011, art. 6°,I.

De súbito vê-se que a LGPD não é um baú, um esconderijo de informações essenciais à sociedade e aos cidadãos.

Pelo contrário: é um manancial de dados que permite, pelo acesso regrado e responsável, a harmonia social e, ao indivíduo, uma vida distante de informações que lhe seriam prejudiciais não fosse o rigor da LGPD.

Ao contrário do que se possa imaginar, a LGPD determina "d*ivulgação dos dados e acesso a aqueles por direito e, mais*"[2], a utilização de recursos públicos, e, mesmo, acesso a dados de difícil obtenção não fosse o respaldo da lei ora enfoque.

Interessante, por assim dizer, é o Capítulo III, Do Procedimento de Acesso à Informação, justamente porque é muito rigoroso e, porque, por ele sabemos que as informações devem ser "imediatas", sem exigências e gratuitas (arts. 10, 11 e incisos)

A Lei n.º 12.527, de 18 de novembro de 2011, que regula o acesso a informações previsto no inciso XXXIII do artigo 5º da Constituição Federal de 1988, é bem anterior à Lei n. 13.709, de 14 de agosto de 2018 (LGPD), ainda assim é a base para a legislação de acesso aos dados pessoais, não tendo sido revogada.

3.2 VAZAMENTO DE DADOS

A violação de dados pessoais constitui, no cenário contemporâneo, um dos fenômenos mais recorrentes e preocupantes no âmbito da proteção da privacidade. A Lei Geral de Proteção de Dados (LGPD) define tratamento de dados de modo amplo, abrangendo desde a coleta até o armazenamento, compartilhamento e eliminação. O vazamento de dados ocorre quando informações pessoais são acessadas, divulgadas ou utilizadas sem o devido consentimento do titular ou em desconformidade com a legislação. Trata-se de evento que pode decorrer de dolo, culpa ou até de erro humano, mas que constantemente compromete a esfera da dignidade da pessoa humana, núcleo axiológico do ordenamento.

No Brasil, casos emblemáticos expõem a vulnerabilidade da proteção de dados, tanto no setor privado quanto no setor público. Em 2021, vieram à tona denúncias de que milhões de dados de cidadãos — inclusive pessoas já falecidas — foram expostos e comercializados em fóruns clandestinos. Informações como CPF, RG, endereços e dados bancários circularam livremente, fomentando fraudes financeiras em larga escala. O impacto desses episódios não se limita ao prejuízo patrimonial: afeta também a confiança social nas instituições, fragiliza a democracia e gera sensação de vulnerabilidade coletiva.

Outro episódio de grande repercussão ocorreu em 2023, quando o grupo hacker Lock Bit invadiu os sistemas da Companhia Estadual de Águas e Esgotos (CEDAE), no Rio de Janeiro. Milhares de documentos internos e dados de usuários foram expostos, demonstrando não apenas a insuficiência de mecanismos técnicos

2 Lei n.º 13.709/2018, Arts. 6º, I e 7º, VI.

de proteção, mas também a vulnerabilidade do próprio setor público, que deveria ser exemplo na observância da LGPD. A divulgação desses dados ampliou a percepção de que a Administração Pública carece de protocolos robustos de segurança da informação, o que se mostra ainda mais grave quando se considera que o Estado detém grande volume de informações sensíveis da população.

No plano internacional, dois casos se destacam. O primeiro é o da Cambridge Analytica, em 2018, quando dados de aproximadamente 87 milhões de usuários do Facebook foram indevidamente utilizados para manipulação de processos eleitorais nos Estados Unidos e no Reino Unido. Esse episódio revelou que a violação de dados pode transcender o campo individual, afetando a própria legitimidade dos regimes democráticos. O segundo é o vazamento da empresa Equifax, em 2017, que expôs dados de cerca de 147 milhões de pessoas nos Estados Unidos, evidenciando que nem mesmo grandes corporações financeiras possuem plena imunidade diante das falhas de segurança digital.

Cumpre destacar que os vazamentos nem sempre decorrem de sofisticados ataques cibernéticos. Estudos indicam que uma parcela significativa dos incidentes resulta de erro humano — negligência no manuseio de informações, falta de capacitação técnica, ou mesmo descuido na adoção de protocolos básicos de segurança. Essa constatação reforça a ideia de que a proteção de dados não é apenas questão tecnológica, mas também cultural e organizacional.

A doutrina já advertia para a banalização dos vazamentos. Stefano Rodotà, precursor do debate europeu sobre privacidade, sustentava que a circulação descontrolada de dados transformaria os indivíduos em meros objetos de vigilância permanente. No Brasil, Danilo Doneda apontava que a ausência de uma cultura de responsabilização conduziria a um ciclo de impunidade, no qual empresas e órgãos públicos não teriam incentivos suficientes para investir em proteção efetiva.

É importante destacar que, como apontam diversos estudiosos, a maior parte dos vazamentos não decorre de ataques cibernéticos sofisticados, mas de falhas humanas.

> A maioria dos vazamentos de dados pessoais ocorre não em razão de sofisticadas práticas criminosas, mas por falhas humanas, decorrentes de desatenção, despreparo técnico ou negligência no cumprimento de protocolos básicos de segurança[3]

Essa constatação revela que a proteção de dados não se limita à adoção de tecnologias avançadas, mas requer cultura organizacional e formação ética dos agentes de tratamento.

Nesse sentido, os vazamentos não devem ser compreendidos como episódios isolados, mas como sintomas de uma falha estrutural. Eles expõem não apenas os

3 DONEDA, Danilo. Da privacidade à proteção de dados pessoais: elementos da formação da autoridade nacional. 2. ed. São Paulo: Thomson Reuters Brasil, 2021.

indivíduos lesados, mas também fragilizam a ordem pública, pois a violação massiva de informações pessoais compromete a segurança nacional, alimenta práticas criminosas e corrói a confiança no sistema jurídico.

Portanto, os casos mencionados não podem ser tratados como meras fatalidades tecnológicas. São, antes, indicadores da necessidade urgente de fortalecimento institucional, de investimento em capacitação profissional e de aplicação rigorosa das sanções previstas na LGPD. A resposta normativa já existe, mas sua eficácia depende de um compromisso político, jurídico e social com a centralidade da dignidade humana no tratamento de dados.

4 DESAFIOS PRÁTICOS NA APLICAÇÃO DA LGPD

A promulgação da Lei Geral de Proteção de Dados Pessoais (LGPD) representou avanço normativo inegável. Entretanto, entre a letra da lei e a realidade social e institucional há um hiato que precisa ser enfrentado. O sucesso da proteção de dados não depende apenas de normas positivadas, mas da capacidade de implementá-las de forma efetiva, o que demanda infraestrutura adequada, vontade política, consciência cultural e maturidade tecnológica.

Os desafios práticos na aplicação da LGPD podem ser agrupados em quatro dimensões principais: cultural, estrutural, tecnológica e institucional.

4.1 OBSTÁCULOS CULTURAIS: A BANALIZAÇÃO DA PRIVACIDADE

Um dos maiores entraves à aplicação plena da LGPD decorre da ausência de uma cultura de proteção de dados na sociedade brasileira. Em um cenário no qual redes sociais, aplicativos de mensagens e plataformas digitais coletam massivamente informações pessoais; grande parte da população demonstra pouca preocupação com o destino desses dados, tratando-os como moeda de troca aparentemente inofensiva.

Essa banalização da privacidade cria terreno fértil para práticas abusivas. O compartilhamento descuidado de informações pessoais — seja ao preencher cadastros online sem leitura dos termos, seja ao consentir automaticamente em políticas de privacidade — enfraquece a autodeterminação informativa. Como aponta Laura Schertel Mendes, "sem consciência da relevância dos dados, não há efetividade no exercício de direitos"[4]. Portanto, a proteção de dados exige, além de normas, formação cidadã que compreenda a privacidade como valor democrático.

4.2 DESAFIOS ESTRUTURAIS: A FRAGILIDADE DA ANPD

Outro obstáculo está no plano institucional. A Autoridade Nacional de Proteção de Dados (ANPD) foi concebida como órgão regulador e fiscalizador, encarregado de

4 MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 90-91

garantir a aplicação uniforme da LGPD. Todavia, desde sua criação, enfrenta críticas quanto à sua autonomia funcional, orçamentária e decisória.

Inicialmente vinculada à Presidência da República, a ANPD careceu de independência administrativa, o que comprometeu sua legitimidade. Embora a Lei n.º 14.460/2022 tenha-lhe conferido natureza autárquica especial, sua estrutura ainda é reduzida frente à complexidade da demanda. Sem equipe técnica robusta, orçamento compatível e mecanismos céleres de atuação sancionatória, a ANPD corre o risco de tornar-se um órgão mais simbólico do que efetivo.

A insuficiência da ANPD revela-se especialmente grave diante da assimetria entre as grandes corporações tecnológicas globais e o poder de regulação estatal. Enquanto empresas multinacionais dispõem de recursos quase ilimitados para explorar dados pessoais, a ANPD luta para consolidar seu papel fiscalizador.

4.3 DEFASAGEM TECNOLÓGICA E SOFISTICAÇÃO DO CIBERCRIME

No campo tecnológico, o desafio se apresenta em duas frentes: (i) a defasagem dos mecanismos de segurança utilizados por órgãos públicos e privados; e (ii) a crescente sofisticação das práticas de cibercriminalidade organizada.

Casos como o ataque hacker ao sistema da CEDAE em 2023 evidenciam que o setor público ainda não dispõe de protocolos adequados de segurança da informação. Muitas vezes, sistemas obsoletos permanecem em uso, vulneráveis a invasões. No setor privado, embora algumas empresas invistam em compliance digital, outras negligenciam a proteção de dados, priorizando redução de custos em detrimento da segurança.

O cibercrime, por sua vez, opera em rede transnacional, valendo-se de fóruns clandestinos, criptografia avançada e softwares de invasão cada vez mais sofisticados. Isso gera um descompasso entre ofensores e defensores, em que os mecanismos protetivos se mostram atrasados em relação às práticas ilícitas.

4.4 A LENIÊNCIA JUDICIAL E A DIFICULDADE DE RESPONSABILIZAÇÃO

Outro desafio diz respeito à resposta do Poder Judiciário. Embora alguns precedentes importantes tenham reconhecido a gravidade dos vazamentos de dados, não raro verifica-se certa leniência judicial, marcada pela demora processual e pela dificuldade em quantificar danos morais coletivos decorrentes de violações massivas.

O STJ, em alguns casos, exige comprovação individualizada de prejuízo, mesmo diante de vazamentos em larga escala, o que dificulta a responsabilização e enfraquece o caráter dissuasório da LGPD. Tal postura diverge com a experiência europeia, na qual a aplicação do GDPR resultou em multas bilionárias contra gigantes da tecnologia, reforçando a seriedade da legislação.

4.5 FORMAÇÃO TÉCNICA E ÉTICA DOS AGENTES DE TRATAMENTO

Por fim, a aplicação efetiva da LGPD depende da capacitação dos agentes públicos e privados responsáveis pelo tratamento de dados. Erros humanos continuam sendo a principal causa de incidentes, expondo ausência de preparo técnico e ético.

É indispensável investir em programas de compliance digital, treinamento contínuo de servidores públicos e empregados do setor privado, bem como difundir boas práticas de governança em proteção de dados. O simples cumprimento formal da lei, desprovido de internalização cultural, é insuficiente.

4.6 SÍNTESE CRÍTICA

Os desafios práticos da LGPD demonstram que a proteção de dados pessoais não é apenas questão normativa, mas sobretudo questão política, institucional e cultural. Enquanto não houver compromisso efetivo do Estado em fortalecer a ANPD, do setor privado em investir em segurança da informação, e da sociedade em valorizar a privacidade, os avanços normativos permanecerão como letra morta.

Portanto, o enfrentamento desses desafios exige um esforço coletivo, que articule a legislação à realidade prática, sob pena de transformar a LGPD em diploma simbólico, incapaz de garantir a proteção da dignidade da pessoa humana no ambiente digital.

5 JURISPRUDÊNCIA E INTERPRETAÇÃO JUDICIAL

O Poder Judiciário desempenha papel essencial na concretização da proteção de dados pessoais no Brasil. A legislação, por si só, não basta: sua efetividade depende da interpretação e aplicação judicial, que deve ser coerente com os fundamentos constitucionais e com os princípios consagrados pela Lei Geral de Proteção de Dados (LGPD).

Nesse contexto, a jurisprudência brasileira revela avanços importantes, mas também contradições que fragilizam a consolidação da proteção de dados como direito fundamental autônomo.

5.1 A FASE ANTERIOR À LGPD: APLICAÇÃO SUBSIDIÁRIA DO MARCO CIVIL DA INTERNET

Antes da vigência da LGPD, o Judiciário brasileiro utilizava como parâmetro normativo o Marco Civil da Internet (Lei n.º 12.965/2014). Esse diploma, ao assegurar a inviolabilidade da intimidade e da privacidade dos usuários, serviu como fundamento para diversas decisões relacionadas a vazamentos, remoção de conteúdo e quebra de sigilo de comunicações.

Entretanto, a ausência de parâmetros específicos para o tratamento de dados pessoais dificultava a uniformidade jurisprudencial. O Judiciário oscilava

entre decisões protetivas e posturas mais flexíveis, muitas vezes justificadas pela necessidade de acesso a informações para investigações criminais.

Exemplo disso é o RHC n.º 117.680/PR, julgado pelo STJ em 2020, em que se admitiu o acesso amplo a dados telemáticos no âmbito de investigação criminal, sem delimitação temporal estrita. À época, a decisão fundamentou-se no Marco Civil da Internet, mas se fosse julgada sob a égide da LGPD, haveria necessidade de maior rigor na proteção da privacidade e no respeito à proporcionalidade.

No RHC n.º 117.680/PR, julgado pelo STJ em 2020, a Corte admitiu o acesso a dados telemáticos para fins de investigação criminal, com base no Marco Civil da Internet, sem exigir delimitação temporal estrita:

> A Lei do Marco Civil da Internet aplica-se às relações privadas, e o art. 10 desse estatuto tem previsão ampla da necessidade de tutela da privacidade de dados pessoais e do conteúdo de comunicações privadas. Além disso, ao tratar do acesso judicial, somente exige limitação temporal no acesso aos registros 'aplicações de internet'. (...) Recurso em habeas corpus improvido.[5] (STJ, RHC 117680/PR, Rel. Min. Nefi Cordeiro, j. 11/02/2020).

A decisão, proferida antes da plena vigência da LGPD, mostra a diferença de rigor entre os diplomas: sob a LGPD, a proporcionalidade e a finalidade legítima deveriam ser observadas com maior intensidade.

Já no STF, a ADPF n.º 872 (2023) consolidou a proteção de dados como direito fundamental autônomo:

> A proteção de dados pessoais constitui direito fundamental autônomo, cujo núcleo é a autodeterminação informativa, essencial para a preservação da dignidade humana e para a efetividade da democracia constitucional[6] (STF, ADPF 872, Rel. Min. ___, j. 2023).

Essa decisão reafirma que a privacidade, no contexto digital, não é mero acessório, mas pilar democrático.

5.2 JURISPRUDÊNCIA PÓS-LGPD: AVANÇOS E RESISTÊNCIAS

Com a entrada em vigor da LGPD, o Judiciário passou a ser instado a interpretar normas específicas sobre tratamento de dados. A partir de então, observa-se movimento de gradual incorporação da proteção de dados como parâmetro decisório, ainda que não isento de contradições.

Um caso paradigmático foi o REsp n.º 1.914.596/RJ, julgado pelo STJ em 2021, que reafirmou a necessidade de observância do sigilo telemático e a gravidade da exposição indevida de dados. A decisão sinalizou avanço na compreensão de que o tratamento irregular de informações pessoais gera danos presumidos à esfera de privacidade do indivíduo.

5 (STJ, RHC 117680/PR, Rel. Min. Nefi Cordeiro, j. 11/02/2020).
6 STF, ADPF 872/DF, Rel. Min. Cármen Lúcia, Tribunal Pleno, j. 14 ago. 2023, DJe 28 ago. 2023.

No âmbito do STF, destaca-se a ADPF n.º 695 (2020)**,** ajuizada contra medida provisória que determinava o compartilhamento massivo de dados de usuários de telefonia com o IBGE. A Corte suspendeu a medida, reconhecendo o risco de violação à intimidade e à autodeterminação informativa. Mais recentemente, a ADPF n.º 872 (2023) consolidou a proteção de dados como direito fundamental autônomo, alinhando o Brasil ao modelo europeu de tutela da privacidade.

5.3 A DIFICULDADE EM RESPONSABILIZAR DANOS COLETIVOS

Apesar de avanços, ainda persistem obstáculos relevantes. O STJ tem demonstrado dificuldade em reconhecer danos morais coletivos decorrentes de vazamentos em larga escala. Em alguns casos, exige-se comprovação individualizada de prejuízo, o que inviabiliza a responsabilização efetiva diante de incidentes que atingem milhões de pessoas.

Tal postura contrasta com o regime europeu, em que o GDPR legitima a imposição de multas administrativas expressivas, aplicadas inclusive contra grandes corporações (a exemplo da multa bilionária aplicada à Meta em 2023).

No Brasil, a ausência de precedentes sancionatórios contundentes enfraquece o efeito dissuasório da LGPD e transmite a mensagem de que o descumprimento pode sair mais barato do que a conformidade.

5.4 RELATÓRIO DO PAINEL LGPD DOS TRIBUNAIS - RAIO - X DO PAINEL LGPD 2024

A partir deste espaço, com satisfação, acompanhamos do Relatório do Painel LGPD dos Tribunais/2024- RAio-X do painel LGPD 2024 e Questões relevantes de aplicação da LGPD pelos tribunais e, propositadamente, não excluímos temas e questões porventura em duplicata de análises advindos do painel 2024, ressaltando a intencionalidade da opção por 2024 posto que o de 2025 já traz referências de teor noviço para estudos futuros.

O Relatório do Painel LGPD dos Tribunais - Raio - X do painel LGPD 2024 como afirma explicitamente acompanha o todo do painel, de que destacamos, de início, o “Panorama geral dos processos analisados” porquanto, por seu relato soberano o campo de batalha jurídica da justiça e das decisões judiciais.

Sabe-se, então, que das 15.921 decisões, a grande maioria foi do setor financeiro (bancos, financeiras e administradoras de...) e que, com envolvimento de dados pessoais estiveram presentes o Direito do Consumidor, Direito Civil, Direito do Trabalho, Direito Constitucional, Direito Processual Civil, Direito de trânsito.

Quanto às decisões da justiça, no Relatório do Painel LGPD dos Tribunais - Raio - X do painel LGPD 2024, seja qual for a peça jurídica, a estatística apresentada corroborando que ainda estamos longe da valorização judicial da LGPD, que o maior percentual incidiu no artigo 5º, II - 27. 37% em 15.921 decisões.

Diga-se que, mesmo nas decisões, há desconhecimento do que pertine à lei da LGPD em abono a fundamentações alheias.

Não assim é o caso relatado no Relatório do Painel LGPD dos Tribunais - Raio - X do painel LGPD 2024, às fls107 e 108, disponível em www.jusbrasil.com.br/jurisprudencia/2840080197 no qual a relatora, Nancy Andrighi, fez valer a lei a analisar e decidir sobre o descredenciamento de um motorista de aplicativo sobre o qual recaíram toneladas de pesos do Código Brasileiro de Trânsito que foram contraposta pelos dispositivos da LGPD, quais sejam: art. 2° § 2°, art. 20, caput § 1° e § 2° tendo em vista que as plataformas de automatizadas aplicam decisões automatizadas com o desprezo indevido do que prevê a LGPD que exige a leitura do lado pessoal do motorista.

Pela quantidade de aplicativos quer-se crer que o caso é interessante, informativo e didático, para todos os envolvidos no feito, assim apresentado em final de fls. 108.

> A decisão também destaca a transparência da LGPD que garante aos titulares o direito à intimação clara, precisa e facilmente acessíveis sobre o tratamento de seus dados, incluindo as razões para o seu descredenciamento. Portanto, o tribunal conclui que um motorista que teve seu perfil profissional suspenso tem o direito de ser informado sobre os motivos e de solicitar a revisão dessa decisão automatizada, assegurando seu direito de defesa. [7]

Valeu a LGPD exigindo fatores objetivos e informações claras e adequadas. LGPD com sua força e decisão adequada.

5.5 RELATÓRIO DO PAINEL LGPD DOS TRIBUNAIS - RAIO - X DO PAINEL LGPD 2025

A análise da aplicação da Lei Geral de Proteção de Dados pelos tribunais brasileiros também pode ser observada a partir do Relatório do Painel LGPD dos Tribunais – Raio-X do painel LGPD 2025, documento que apresenta levantamento estatístico e qualitativo acerca das decisões judiciais relacionadas à proteção de dados pessoais.

Após a análise do panorama referente ao ano de 2024, torna-se relevante registrar que o relatório referente a 2025, especialmente no Caderno 4, apresenta reflexões conclusivas relevantes sobre a evolução da aplicação da LGPD no âmbito do Poder Judiciário.

Conforme exposto no Relatório do Painel LGPD dos Tribunais (2025), observa-se que a jurisprudência brasileira tem incorporado gradualmente os princípios da Lei Geral de Proteção de Dados às decisões judiciais. Todavia, o próprio relatório aponta que ainda persistem divergências interpretativas, especialmente no que se refere à extensão da responsabilidade civil e à caracterização do dano moral decorrente do tratamento irregular de dados pessoais.

7 Relatório do Painel LGPD dos Tribunais - Raio - X do painel LGPD 2024, fls.108.

O relatório evidencia que, embora se observe crescimento significativo no número de decisões que mencionam a LGPD, a consolidação de uma jurisprudência plenamente estruturada ainda se encontra em processo de amadurecimento. Esse movimento revela que o direito à proteção de dados pessoais, apesar de constitucionalizado pela Emenda Constitucional n.º 115/2022, ainda atravessa fase de sedimentação interpretativa no âmbito judicial.

Nesse contexto, o levantamento estatístico e analítico realizado pelo Painel LGPD dos Tribunais constitui importante instrumento de observação empírica da evolução jurisprudencial brasileira, permitindo identificar tendências interpretativas, lacunas normativas e desafios práticos na aplicação da legislação de proteção de dados.

5.6 O PAPEL DO STF: A CONSTITUCIONALIZAÇÃO DA PROTEÇÃO DE DADOS

A atuação do Supremo Tribunal Federal tem sido decisiva para consolidar a proteção de dados como direito fundamental. A já mencionada Emenda Constitucional n.º 115/2022 conferiu densidade formal ao tema, mas foi o STF que deu efetividade prática ao reconhecer a proteção de dados como elemento essencial à dignidade da pessoa humana e à democracia.

Na ADI n.º 6.387 (2020), a Corte suspendeu a medida provisória que autorizava o compartilhamento irrestrito de dados com o IBGE, enfatizando a necessidade de proporcionalidade, adequação e finalidade legítima. Essa decisão reforçou o entendimento de que o Estado não pode tratar dados pessoais de forma indiscriminada, mesmo sob justificativas de interesse público.

Esses precedentes indicam uma evolução no sentido de reconhecer a autodeterminação informativa como núcleo essencial do direito à privacidade, impondo limites à atuação estatal e privada no tratamento de dados.

5.7 SÍNTESE CRÍTICA DA JURISPRUDÊNCIA BRASILEIRA

A análise da jurisprudência permite identificar três tendências principais:

a) Avanço gradual na consolidação da proteção de dados como direito fundamental, sobretudo após a EC n.º 115/2022;

b) Inconsistência na responsabilização de danos coletivos, em razão da exigência de comprovação individualizada;

c) Atuação central do STF, que tem fixado parâmetros constitucionais protetivos, em contraste com a hesitação do STJ em impor reparações mais amplas.

O desafio, portanto, é consolidar uma jurisprudência coerente e protetiva, capaz de efetivar os princípios da LGPD e de superar a cultura de impunidade diante dos vazamentos.

6 CONSIDERAÇÕES FINAIS

A proteção de dados pessoais no Brasil constitui, ao mesmo tempo, conquista normativa e desafio civilizatório. A positivação constitucional promovida pela Emenda Constitucional n.º 115/2022, que inseriu no rol do art. 5º o direito fundamental à proteção de dados, consolidou juridicamente um percurso iniciado com o Marco Civil da Internet (Lei n.º 12.965/2014) e fortalecido pela Lei Geral de Proteção de Dados (Lei n.º 13.709/2018). Contudo, entre a norma e a realidade há uma distância que precisa ser superada por meio de instrumentos institucionais, culturais e políticos.

Os exemplos de vazamentos massivos de dados revelam a insuficiência das medidas adotadas até o momento. Seja em episódios nacionais, como a exposição de milhões de registros de brasileiros em fóruns clandestinos ou o ataque hacker à CEDAE em 2023, seja em episódios internacionais, como o escândalo da Cambridge Analytica ou o vazamento da Equifax, a mensagem é clara: os dados se transformaram na moeda mais valiosa da era digital e, portanto, também em alvo preferencial de práticas ilícitas. Proteger dados é proteger patrimônio, mas, sobretudo, é proteger pessoas e sua dignidade.

Nesse contexto, a LGPD representa mais que uma lei: é um marco ético e político. Seu núcleo principiológico — finalidade, necessidade, adequação, transparência, segurança e responsabilização e sobretudo boa-fé — traduz o compromisso de colocar o ser humano no centro da regulação digital. No entanto, a efetividade desse compromisso depende de condições concretas: o fortalecimento da Autoridade Nacional de Proteção de Dados (ANPD), a consolidação de uma jurisprudência protetiva e a construção de uma cultura cidadã de privacidade.

O fortalecimento institucional da ANPD é imperativo. Sem autonomia decisória, orçamento robusto e capacidade técnica ampliada, a autoridade corre o risco de permanecer como órgão simbólico, incapaz de enfrentar a assimetria entre grandes corporações tecnológicas e o cidadão comum. No direito comparado, o sucesso do GDPR europeu não decorre apenas do rigor da norma, mas também da atuação firme das autoridades de proteção, capazes de impor multas bilionárias e de influenciar políticas empresariais em escala global. O Brasil precisa trilhar caminho semelhante, sob pena de transformar sua lei em instrumento meramente declaratório.

A jurisprudência brasileira também precisa avançar. O Supremo Tribunal Federal tem desempenhado papel essencial na fixação de parâmetros constitucionais, como se viu na ADI n.º 6.387 (2020) e na ADPF n.º 872 (2023). Todavia, no Superior Tribunal de Justiça ainda se verificam decisões que dificultam a responsabilização coletiva, exigindo comprovação individual de danos em casos de vazamentos massivos. Essa postura precisa ser revista, sob pena de perpetuar a sensação de impunidade. O reconhecimento de danos morais coletivos, bem

como a aplicação de indenizações expressivas, são instrumentos indispensáveis para conferir efetividade dissuasória à LGPD.

Para além da esfera normativa e institucional, há um desafio cultural: superar a banalização da privacidade. No cotidiano, muitos cidadãos ainda tratam seus dados como se fossem bens de pouca importância, cedendo-os indiscriminadamente a aplicativos, plataformas e cadastros digitais. Essa postura fragiliza a própria autodeterminação informativa, pois impede o exercício consciente dos direitos previstos na LGPD. É necessário promover formação cidadã, que envolva desde a educação básica até programas de capacitação profissional, de modo a consolidar uma cultura de proteção de dados.

Em perspectiva filosófica, a proteção de dados é inseparável da própria noção de dignidade humana. Assim como no passado a luta pela liberdade política e pelos direitos civis marcou o constitucionalismo, hoje a luta pelo controle sobre as informações pessoais define os contornos da cidadania digital. Negligenciar a proteção de dados é abrir espaço para novas formas de dominação — econômica, política e social — que se valem do conhecimento íntimo da vida das pessoas para influenciar decisões, manipular comportamentos e fragilizar democracias.

Portanto, proteger dados é proteger a democracia. É assegurar que a pessoa humana não seja reduzida a objeto de vigilância e manipulação, mas permaneça como sujeito de direitos, livre e autônomo. A LGPD, embora jovem e ainda em construção, representa um instrumento poderoso para essa finalidade. Mas sua força não reside apenas em seu texto: depende da atuação vigilante da sociedade civil, do compromisso das instituições e da sensibilidade ética dos operadores do Direito.

Conclui-se, assim, que o futuro da proteção de dados no Brasil não será definido apenas pelas normas, mas pela responsabilidade coletiva de aplicá-las, aprimorá-las e defendê-las. Só quando a proteção de dados for compreendida como dimensão inarredável da dignidade da pessoa humana é que poderemos afirmar que o país avançou verdadeiramente no caminho da cidadania digital.

REFERÊNCIAS

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília: Senado Federal, 1988.

BRASIL. **Emenda Constitucional n.º 115**, de 10 de fevereiro de 2022. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais. Diário Oficial da União, Brasília, DF, 11 fev. 2022.

BRASIL. **Lei n.º 12.965**, de 23 de abril de 2014. **Marco Civil da Internet**. Diário Oficial da União, Brasília, DF, 24 abr. 2014.

BRASIL. **Lei n.º 13.709**, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Diário Oficial da União, Brasília, DF, 15 ago. 2018.

BRASIL. **Lei n.º 13.853**, de 8 de julho de 2019. Altera a Lei n.º 13.709/2018. Diário Oficial da União, Brasília, DF, 9 jul. 2019.

BRASIL. **Lei n.º 14.460, de 2022. Altera a estrutura da Autoridade Nacional de Proteção de Dados (ANPD)**. Diário Oficial da União, Brasília, DF, 28 set. 2022.

UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016. **Regulamento Geral sobre a Proteção de Dados (GDPR)**. Jornal Oficial da União Europeia, 4 maios 2016.

BRASIL. Supremo Tribunal Federal. **Arguição de Descumprimento de Preceito Fundamental n.º 872**. Rel. Min. ___, Tribunal Pleno, julgado em 2023.

BRASIL. Supremo Tribunal Federal. **Ação Direta de Inconstitucionalidade n.º 6.387**. Rel. Min. Rosa Weber, Tribunal Pleno, julgado em 07 maio 2020.

BRASIL. Supremo Tribunal Federal. **Arguição de Descumprimento de Preceito Fundamental n.º 695**. Rel. Min. Rosa Weber, Tribunal Pleno, julgado em 07 maio 2020.

BRASIL. Superior Tribunal de Justiça. **Recurso em Habeas Corpus n.º 117.680/PR**. Rel. Min. Nefi Cordeiro, 6ª Turma, julgado em 11 fev. 2020.

BRASIL. Superior Tribunal de Justiça. Recurso Especial n.º 1.914.596/RJ. Rel. Min. Nancy Andrighi, 3ª Turma, julgado em 09 mar. 2021.

ARAÚJO, Marcelo Melo Barreto de. ***Proteção de Dados Pessoais no Brasil***. Belo Horizonte: Fórum, 2022.

DONEDA, Danilo. ***Da privacidade à proteção de dados pessoais: elementos da formação da autoridade nacional***. 2. ed. São Paulo: Thomson Reuters Brasil, 2021.

MENDES, Laura Schertel. ***Privacidade, proteção de dados e defesa do consumidor na era digital.*** São Paulo: Revista dos Tribunais, 2019.

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

BYGRAVE, Lee A. ***Data Privacy Law: An International Perspective***. Oxford: Oxford University Press, 2014.

PAINEL LGPD DOS TRIBUNAIS. **Relatório do Painel LGPD dos Tribunais: raio-X do painel LGPD 2025**. Brasília: Painel LGPD dos Tribunais, 2024. Acesso em 20/02/2026.

PAINEL LGPD DOS TRIBUNAIS. **Relatório do Painel LGPD dos Tribunais: raio-X do painel LGPD 2025**. Brasília: Painel LGPD dos Tribunais, 2025. Acesso em 20/02/2026.