Revista | Direitos Sociais e Políticas Públicas | Unifafibe

EROSÃO DO AUTOCONTROLE E A TUTELA GARANTISTA: A NATUREZA JURÍDICA DA AUTODETERMINAÇÃO INFORMATIVA COMO DIREITO DA PERSONALIDADE SOB A ÓTICA DA FISCALIZAÇÃO COMPARADA (ANPD E DPC)

EROSION OF SELF-CONTROL AND GUARANTEE-BASED PROTECTION: THE LEGAL NATURE OF INFORMATIONAL SELF-DETERMINATION AS A PERSONALITY RIGHT FROM THE PERSPECTIVE OF COMPARATIVE SUPERVISION (ANPD AND DPC)

Recebido em	08/09/2025
Aprovado em:	18/11/2025

Marcelo Negri Soares[1]
Dirceu Pereira Siqueira[2]
Alender Max de Souza Moraes[3]

RESUMO

Este artigo é fruto de pesquisa em que se investiga a origem, evolução, desafios e impactos sobre a autodeterminação informativa e a proteção de dados pessoais na sociedade digital, com foco nas redes sociais. Com esteio em uma metodologia rigorosa, a pesquisa inclui revisão sistemática da literatura e ferramentas de inteligência artificial como o NotebookLM para análise documental. Os materiais de pesquisa são, em sua maioria, decisões proferidas em execução de fiscalização pela Autoridade Nacional de Proteção de Dados (ANPD) do Brasil e pela Data Protection Commission (DPC) da Irlanda, envolvendo

[1] Professor do Mestrado e Doutorado em Direito da Unicesumar. Advogado e contabilista. Professor Visitante da Coventry University (UK).
[2] Pós Doutor em Direito pela Universidade de Coimbra. Doutor e Mestre em Sistema Constitucional de Garantia de Direitos pelo Instituição Toledo de Ensino. Docente do Centro Universitário Unifafibe. Advogado.
[3] Doutorando em Direito (UNICESUMAR). Mestre em Direito Processual Civil e Cidadania (UNIPAR). Advogado., Auditor de Controle Interno e Professor da UEMS.

Revista | Direitos Sociais e Políticas Públicas Unifafibe

violações a direitos da personalidade nas práticas de tratamento de dados do TikTok e da Meta (Facebook, Instagram e WhatsApp). A análise das decisões baseou-se no framework de Análise de Impacto Regulatório (AIR), que decompôs cada caso em problema regulatório, análise de políticas, impactos e estratégias de fiscalização. São apresentados os resultados da revisão de literatura e dos estudos de caso na forma de quadros, a partir dos quais se identifica a capacidade do indivíduo de gerir o fluxo de informações (autocontrole). Assim, ficou patente a erosão de informações sensíveis frente à assimetria de poder, somada à falta de lealdade por parte das grandes plataformas de tecnologia. Este trabalho apontou a dupla natureza jurídica da autodeterminação informativa: em sua dimensão subjetiva (autocontrole), configura-se como um direito da personalidade; por outro lado, na sua dimensão garantista, em seus papéis sociais (envolvendo, por exemplo, direitos do consumidor, da criança ou do idoso, os quais são efetivados pelo controle externo, seja judicial ou administrativo), um direito da pessoa. Ao fim, propõem-se melhorias buscando fortalecer a LGPD e o sistema regulatório brasileiro, em três frentes: aprimoramento legislativo (substancial), fortalecimento dos mecanismos de controle (processual) e consolidação da infraestrutura institucional (estratégica).

Palavras-chave: Autodeterminação informativa; Fiscalização; Proteção de dados; Redes sociais; Tutela efetiva.

ABSTRACT

This article is the result of research investigating the origin, evolution, challenges, and impacts on informational self-determination and the protection of personal data in the digital society, focusing on social networks. The research uses a rigorous methodology that includes a systematic literature review and the use of Artificial Intelligence tools such as NotebookLM for document analysis. The research corpus consists of preferred decisions in oversight procedures of the Brazilian National Data Protection Authority (ANPD) and the Irish Data Protection Commission (DPC), involving violations of personality rights in the data processing practices of TikTok and Meta (Facebook, Instagram, and WhatsApp). The analysis of the decisions was based on the Regulatory Impact Analysis (RIA) framework, which decomposed each case into a regulatory problem, policy analysis, impacts, and enforcement strategies. The results of the literature review and case studies are presented in the form of tables, from which the individual's capacity to manage the flow of information (self-control) is identified. Thus, the erosion of sensitive information in the face of power asymmetry coupled with a lack of loyalty on the part of large technology platforms became evident. This work pointed to the dual legal nature of informational self-determination: in its subjective dimension (self-control), it is configured as a personality right; on the other hand, in its guarantee dimension, in its

Revista | Direitos Sociais e Políticas Públicas Unifafibe

social roles (involving, for example, consumer, child, or elderly rights, which are enforced through external control, whether judicial or administrative), it is a right of the person. Finally, improvements are proposed to strengthen the LGPD (Brazilian General Data Protection Law) and the Brazilian regulatory system, in three areas: legislative improvement (substantive), strengthening of control mechanisms (procedural), and consolidation of institutional infrastructure (strategic).

Keywords: Informational self-determination; Oversight; Data protection; Social networks; Effective legal protection.

INTRODUÇÃO

A autodeterminação informativa é um direito fundamental de terceira geração que concede ao indivíduo o poder, ativo e reativo, de controlar a coleta, o tratamento, a circulação e a utilização de seus dados pessoais. Ao longo da origem e desenvolvimento desse instituto buscou-se reconhecer que todo indivíduo tem o direito de exercer controle sobre o ciclo de vida de seus dados pessoais, abrangendo sua coleta, armazenamento, processamento e disseminação. Desde a metade do Século XX, esse direito vem ganhando proeminência em decisões judiciais, comentários doutrinários e legislações especiais.

No entanto, em razão da assimetria de poder (econômico e informacional) entre indivíduos e entidades (públicas ou privadas), o autocontrole, ou seja, a capacidade do indivíduo de gerir o fluxo de informações, foi sendo erodido.

A erosão da autonomia individual no ambiente das redes sociais decorre diretamente da assimetria de poder e da opacidade algorítmica, que tornam a decisão baseada no consentimento uma "ficção jurídica", inviabilizando o autocontrole. Neste contexto,garantistao garantista — exercida pela fiscalização e tutela coletiva da Autoridade Nacional de Proteção de Dados (ANPD) — atua não apenas como um complemento, mas como um substituto estrutural da racionalidade individual. Ela reconstrói a efetividade do direito ao impor deveres de lealdade, transparência e Privacy by Design às plataformas, corrigindo as falhas sistêmicas do mercado e garantindo que o ambiente de tratamento de dados seja fundamentalmente equitativo e seguro. A tutela garantista, portanto, substitui o autocontrole ineficaz do usuário por um controle externo

Revista | Direitos Sociais e Políticas Públicas Unifafibe

e preventivo da Autoridade, o que, paradoxalmente, reconstrói a base mínima para que qualquer exercício autônomo futuro seja verdadeiramente informado e livre de vícios.

Não obstante a necessidade e importância da intervenção garantista, esta substituição da autonomia individual possui limites bem delineados, sob pena de incorrer em um paternalismo regulatório que nega a própria essência do direito da personalidade. O limite da intervenção reside em assegurar as condições de possibilidade do exercício autônomo, e não em ditar a execução da escolha do titular. O papel da ANPD é estabelecer o compliance obrigatório para as empresas, forçando-as a criar um ambiente de lealdade informacional. Contudo, o "direito à última palavra" sobre o uso de seus dados deve permanecer com o titular, mesmo que ele opte por uma exposição que o regulador considere de risco. A dimensão garantista, em suma, deve restaurar a capacidade de escolha, mas não eliminar o ato de escolher, preservando a essência subjetiva do direito à autodeterminação informativa.

Esse cenário justifica a relevância de aprofundar pesquisas acadêmicas sobre como enfrentar um modelo de negócio assentado sobre imensa captura, armazenamento e processamento de dados e informações digitais. Esse modelo é engendrado pelas chamadas *Big Techs*, grandes empresas de tecnologia que dominam o mercado global e refinam estratégias de manipulação de comportamentos humanos.

Aquele contexto motivou o desenvolvimento inclusive de tema de tese de doutoramento, com área de concentração em Direitos da Personalidade, do qual esse escrito é uma continuidade da pesquisa. O cerne da questão aqui posta é responder: quais são as violações à autodeterminação informativa nas práticas de tratamento de dados por redes sociais fiscalizadas pela ANPD no Brasil e pela *Data Protection Commission* na Irlanda (DPC, Irlanda)?

O presente ensaio é uma continuidade da pesquisa sobre novas tecnologias e os direitos da personalidade (Soares, Kauffman, Chao, Saad, 2020). A questão surgiu após realização de uma revisão sistemática de literatura que identificou uma lacuna de estudos tanto na literatura nacional quanto na internacional que abordem especificamente as violações da autodeterminação informativa nas práticas de tratamento de dados das

Revista | Direitos Sociais e Políticas Públicas Unifafibe

redes sociais fiscalizadas pela Autoridade Nacional de Proteção de Dados (ANPD). Preencher esse *gap* ofereceu uma oportunidade para a produção de pesquisas de base que auxiliem a compreender as causas dessas violações e o modo de fiscalização da autoridade brasileira de proteção de dados.

O estudo visou investigar os impactos causados pelas novas tecnologias referentes ao direito da personalidade à autodeterminação informativa e os desafios à proteção de dados pessoais digitais no contexto da sociedade de vigilância, tema relevante dentro do Programa porque alinhado à Linha de Pesquisa Instrumentos de efetivação dos Direitos da Personalidade. Ele buscou seguir os seguintes objetivos específicos: i) examinar a evolução histórico-normativa do direito à autodeterminação informativa no ordenamento jurídico brasileiro, desde sua concepção doutrinária até sua incorporação pela Emenda Constitucional n. 115/2022; ii) identificar procedimentos de fiscalização e as principais decisões da Autoridade Nacional de Proteção de Dados (ANPD) relacionadas ao tratamento de dados pessoais e proferidas em face às redes sociais no Brasil; iii) analisar as decisões proferidas nos procedimentos de fiscalização instaurados junto à ANPD, em face de redes sociais como WhatsApp, Facebook e Instagram, verificando as causas de violações ao direito à autodeterminação informativa; iv) identificar as interseções entre as decisões brasileiras e as decisões análogas proferidas no âmbito da Autoridade Irlandesa de Proteção de Dados (DPC-Irlanda) proferidas em face das mesmas redes sociais investigadas nos procedimentos brasileiros, e, por fim; v) propor melhorias normativas para aprimorar a proteção do direito à autodeterminação informativa dos usuários brasileiros de redes sociais.

Para atingir aqueles objetivos realizou-se uma segunda revisão sistemática de literatura com a finalidade de examinar o estado da arte da evolução histórico-normativa do direito à autodeterminação informativa no ordenamento jurídico brasileiro, desde sua concepção doutrinária até sua incorporação pela Emenda Constitucional n. 115/2022. E, foi realizado o Estudos de Caso de 12 decisões (5 da ANPD e 7 da DPC-Irlanda) que analisavam e respondiam a situações de violações à autodeterminação informativa nas

Revista | Direitos Sociais e Políticas Públicas Unifafibe

práticas de tratamento de dados por redes sociais fiscalizadas pela ANPD no Brasil e pela *Data Protection Commission* na Irlanda (DPC-Irlanda).

1. METODOLOGIA

O caminho percorrido para a pesquisa foi o método dedutivo (método de abordagem geral). O presente estudo foi estruturado em um protocolo de pesquisa de oito etapas (Quadro 1), partindo do estabelecimento de premissas gerais (como os princípios da autodeterminação informativa, LGPD e GDPR) para a construção argumentativa, confronto com a prática administrativa (ANPD e DPC), e validação da conclusão; bem como, foram empregados quatro procedimentos metodológicos complementares, utilizados de forma integrada: histórico, comparativo, monográfico, aplicando, por fim, a análise de impacto regulatório (AIR).

O método histórico foi utilizado para investigar a evolução e as raízes da autodeterminação informativa e sua influência na sociedade atual (Tepedino, Pereira, 2024). Foi aplicado no desenvolvimento do Capítulo 2 para analisar a trajetória normativa no Brasil, desde 1988 (Constituição Federal) até 2025, passando pelo Marco Civil da Internet (2014), LGPD (2018) e a Emenda Constitucional n. 115/2022.

No aspecto comparativo, o método em específico foi empregado para examinar indivíduos, classes, fenômenos ou fatos com o intuito de identificar similaridades e diferenças. Foi essencial para a análise comparada das estratégias de ação entre a Autoridade Nacional de Proteção de Dados (ANPD) no Brasil e a Data Protection Commission (DPC) na Irlanda.

Aplicado também o método monográfico para o estudo aprofundado de casos envolvendo redes sociais, examinando todos os fatores que os influenciam, como práticas de tratamento de dados, mecanismos de consentimento e procedimentos de transparência.

Por fim, ganhou importância a análise de impacto regulatório (AIR) como procedimento aplicado como *framework* analític (Justen Filho, 2020; Warren, Brandeis, 1890) A AIR é uma ferramenta amplamente utilizada na Europa, e seus componentes

Revista | Direitos Sociais e Políticas Públicas Unifafibe

serviram de parâmetro para o método comparativo. Ele permitiu a decomposição das decisões da DPC e da ANPD em componentes funcionais: Problema Regulatório, Análise de Políticas Regulatórias, Análise de Impactos, seja da análise estratégico na implementação ou fiscalizatório e de acompanhamento monitorado. O artigo legitima o uso do AIR como uma ferramenta de Direito Público e Regulatório para a decomposição e análise das decisões da ANPD (uma autarquia federal), demonstrando que o framework não é apenas uma escolha metodológica, mas uma lente conceitual alinhada com as melhores práticas de análise regulatória no país. Na mesma linha, embora trate de autodeterminação informativa (conceito mais recente), é fundamental lembrar que Warren e Brandeis estão conectados com a evolução histórica dos Direitos da Personalidade, pois eles estabeleceram a base teórica de onde a proteção da esfera íntima evoluiu para incluir a proteção de dados na era digital.

A pesquisa utilizou a plataforma *NotebookLM* (um *Large Language Model* - LLM) como ferramenta principal para a Revisão Sistemática de Literatura (RSL) e para a elaboração dos Estudos de Caso. O *NotebookLM* foi usado para a extração profunda de conteúdo das decisões, respondendo a quatro questões-chave baseadas no *framework* AIR (problema regulatório, políticas regulatórias, impactos e estratégias de ação). E, garantia de Rastreabilidade: para mitigar o risco da "caixa-preta" dos LLMs, um rigoroso protocolo de verificação humana foi implementado. A ferramenta gera notas numéricas que mapeiam o trecho exato do documento original (referências por parágrafo, e.g.,), garantindo uma rastreabilidade e verificabilidade hipergranular dos achados.

Assim, foram realizadas duas RSLs com protocolos específicos. Na chamada primeira fase (pré-qualificação) investigou-se a dimensão da literatura, a originalidade e ineditismo da tese. Já na segunda fase (desenvolvimento) buscou-se compreender a origem e o desenvolvimento da autodeterminação informativa, resultando na análise de 109 documentos. O *corpus* empírico foi composto por decisões proferidas em procedimentos administrativos de natureza fiscalizatória pela ANPD (Brasil) e decisões publicadas pela DPC (Irlanda), entre 2020 e 2025, focadas em redes sociais como *WhatsApp, Facebook* e *Instagram*.

Revista | Direitos Sociais e Políticas Públicas Unifafibe

Numa etapa inicial, o método histórico foi essencial para traçar a evolução da autodeterminação informativa no ordenamento jurídico brasileiro, desde seus alicerces conceituais até a consagração constitucional. Concomitantemente, o método histórico foi combinado com o método comparativo, utilizando a estrutura da Análise de Impacto Regulatório (AIR) para contrastar essa trajetória brasileira com o desenvolvimento e as tendências internacionais. O objetivo era construir uma base sólida de conhecimento e identificar as intersecções teóricas entre as jurisdições.

A segunda fase concentrou-se na análise da prática administrativa. O método monográfico foi aplicado para gerar dados empíricos detalhados a partir de casos concretos de fiscalização, fornecendo a base factual necessária para o estudo. Esses dados monográficos foram então articulados com a estrutura da AIR, permitindo a sistematização de todos os casos estudados (ANPD e DPC) dentro de um framework regulatório unificado. Essa conjugação metodológica foi crucial para traduzir a narrativa administrativa das decisões em componentes funcionais de problemas, políticas e impactos.

A fase final consistiu na integração coerente dos quatro métodos (histórico, comparativo, monográfico e AIR). Essa síntese permitiu a formulação do diagnóstico conclusivo sobre a crise do autocontrole e a necessidade da tutela garantista. As propostas de melhoria foram desenvolvidas a partir dessa integração, sendo validadas tanto pelas experiências regulatórias internacionais (analisadas via AIR) quanto pela demonstração da viabilidade prática fundamentada nas evidências empíricas extraídas dos estudos monográficos.

A aplicação do framework de Análise de Impacto Regulatório (AIR) foi fundamental para conferir o rigor metodológico exigido por periódicos de ponta, permitindo a decomposição sistemática das decisões administrativas estudadas. A título de ilustração explícita, tomamos como estudo de caso a decisão da Data Protection Commission (DPC) da Irlanda contra a Meta Platforms Ireland Ltd. (referente aos serviços do Facebook e Instagram), na qual a Autoridade questionou o uso inadequado da base legal de "Execução

Revista | Direitos Sociais e Políticas Públicas Unifafibe

de Contrato" (Art. 6º, n.º 1, alínea b, do GDPR) para o tratamento de dados com fins de publicidade comportamental (Branco, Teffé, Fernandes, 2024).

Por meio do AIR, o caso é traduzido em quatro vetores: o Problema Regulatório é identificado como a imposição de uma publicidade altamente invasiva sob o modelo *take-it-or-leave-it*, o que vicia a autonomia do usuário; a Análise de Políticas se concentra no julgamento de que a publicidade personalizada, embora comercialmente desejável pela plataforma, não é objetivamente necessária para a prestação do serviço principal da rede social (conexão e feed de conteúdo), invalidando a base legal empregada.

Essa decomposição do caso, guiada pelo AIR, permite ao artigo ir além da descrição dos fatos. Os Impactos da conduta da Meta são claramente mapeados como a violação do princípio da lealdade (Fairness) e a consequente perda de controle do titular, validando a tese central da erosão do autocontrole individual. Em resposta, as Estratégias de Fiscalização da DPC consistiram em ordens de conformidade e aplicação de multas substanciais, que serviram para reforçar que o modelo de negócio das plataformas deve se curvar à lei, e não o contrário. Ao utilizar a AIR, o trabalho demonstra cientificamente que as autoridades reguladoras, tanto a irlandesa quanto a brasileira (ANPD), estão convergindo na identificação de um problema comum – a falência do consentimento individual – e na adoção de um modelo garantista de tutela, onde a imposição regulatória externa é o único mecanismo capaz de restaurar as condições mínimas de lealdade no tratamento de dados.

Essa estrutura metodológica assegurou que a pesquisa fosse embasada em evidências, sistemática e objetiva, conforme os critérios exigidos para uma tese de doutorado. A revisão sistemática de literatura levou ao levantamento da premissa de que a autodeterminação informativa é insuficiente para garantir a proteção de direitos da personalidade. A autodeterminação informativa, um direito fundamental de origem germânica, transcende a mera esfera da privacidade, estabelecendo o poder de controle sobre o fluxo de dados (Doneda, 2006). No ambiente das redes sociais, a capacidade de autocontrole do indivíduo é uma ficção jurídica diante da assimetria informacional (Tepedino, Pereira, 2024). Essas premissas substanciais foram corroboradas pelos

Revista | Direitos Sociais e Políticas Públicas Unifafibe

achados da RSL, especialmente porque: a) a literatura estrangeira (principalmente da União Europeia) já evidenciava o reconhecimento de que a autodeterminação informativa é insuficiente para proteger plenamente os direitos da personalidade; b) os estudos internacionais estavam migrando o foco da autodeterminação informativa para análises situacionais e estratégias de ação mais específicas, alinhadas ao contexto regulatório europeu avançado.

A análise sistemática da literatura permitiu identificar onze temáticas centrais que compõem a discussão contemporânea sobre o assunto: comodificação dos dados pessoais; vigilância e compartilhamento não autorizado; insuficiência normativa pré-LGPD; manipulação comportamental; reconhecimento da proteção de dados como direito da personalidade; desenvolvimento da cultura democrática digital; responsabilidade civil das plataformas; direito ao esquecimento; proteção de menores no ambiente digital; combate à desinformação e, por fim, a regulamentação do cancelamento virtual.

2. RESULTADOS PRELIMINARES DA COLETA DE DADOS

Os estudos de caso de decisões da *Data Protection Commission* (DPC) da Irlanda, que atuou como Autoridade Supervisora Principal para a *Meta* (*Facebook, Instagram, WhatsApp*) na União Europeia, revelaram uma série de violações sistêmicas e graves ao Regulamento Geral de Proteção de Dados (GDPR). As investigações da DPC focaram principalmente na falha em garantir a autodeterminação informativa dos usuários, devido à assimetria de poder e à falta de transparência. A metodologia utilizada pela DPC para analisar as decisões se baseou no *framework* de Análise de Impacto Regulatório (AIR), que decompôs cada caso em Problema Regulatório, Análise de Políticas, Impactos e Estratégias de Fiscalização.

Os achados da DPC confirmam que a dimensão individual da autodeterminação informativa é destituída de efetividade nas práticas das redes sociais, exigindo a intervenção enérgica de autoridades reguladoras para enfrentar a assimetria de poder e a falta de lealdade e transparência das grandes plataformas de tecnologia.

Revista | Direitos Sociais e Políticas Públicas Unifafibe

Os estudos de caso das decisões da Autoridade Nacional de Proteção de Dados (ANPD) no Brasil, conduzidos por meio da metodologia de Análise de Impacto Regulatório (AIR), focaram em procedimentos fiscalizatórios contra grandes plataformas digitais, como WhatsApp, Meta (Facebook/Instagram) e TikTok. As análises da ANPD revelaram falhas sistêmicas que violam consistentemente a Lei Geral de Proteção de Dados – LGPD (BRASIL, 2018) e comprometem a autodeterminação informativa dos usuários brasileiros, especialmente os mais vulneráveis.

As investigações da ANPD também confirmam que a dimensão individual da autodeterminação informativa é destituída de efetividade diante das práticas de tratamento de dados pelas redes sociais, exigindo uma ação positiva e enérgica da autoridade reguladora para proteger os direitos, especialmente em um ambiente marcado pela assimetria de poder e pela falta de lealdade por parte das grandes plataformas de tecnologia.

3. AUTODETERMINAÇÃO INFORMATIVA: EVOLUÇÃO

A segunda Revisão Sistemática de Literatura (RSL-II) foi realizada na fase de desenvolvimento da pesquisa com o objetivo de compreender a origem e o desenvolvimento da autodeterminação informativa. Os resultados dessa revisão sistemática podem ser sintetizados em achados quantitativos, no marco conceitual decisivo e na identificação dos desafios contemporâneos à efetividade do direito.

3.1 Coleta de dados e resultados quantitativos

A RSL-II foi conduzida em maio de 2025, utilizando o Biblioteca Digital Brasileira de Teses e Dissertações (BDTD),[4] o Catálogo de Teses e Dissertações da CAPES[5] e o Periódicos Capes.[6] A busca inicial localizou no total 346 documentos (118 do Catálogo

[4] Biblioteca Digital Brasileira de Teses e Dissertações (BDTD). Link: http://200.130.0.112/bdtd/. Acesso em: 07.11.2025.
[5] Catálogo de Teses e Dissertações da CAPES. Link: https://catalogodeteses.capes.gov.br/catalogo-teses/#!/. Acesso em: 07.11.2025.
[6] Periódicos Capes. Link: https://www.periodicos.capes.gov.br/. Acesso em: 07.11.2025.

Revista | Direitos Sociais e Políticas Públicas Unifafibe

CAPES, 83 artigos e 145 do BDTD). Após a aplicação de filtros (acesso aberto, revisado pelos pares e área de ciências sociais aplicadas), restaram 294 documentos. E com a exclusão de duplicados (117) e aqueles não relacionados ao objeto de investigação (48), a pesquisa se baseou na análise de 109 documentos (Quadro 14). A análise desses 109 documentos foi realizada com auxílio do *Large Language Model* (LLM) *NotebookLM*, que gerou a Linha do Tempo para mapear a gênese e o amadurecimento dos institutos jurídicos, como a autodeterminação informativa e a proteção de dados.

3.2 Marcos conceituais, históricos e legais

A análise da literatura levou a constatação que a capacidade de se autodeterminar informativamente é vista como um elemento essencial para a construção da subjetividade e para a liberdade no desenvolvimento da personalidade. Quando uma pessoa não consegue saber quais de suas informações pessoais são apropriadas e como estão sendo usadas, sua autonomia é comprometida, dificultando o planejamento e a tomada de decisões no momento certo.

E que a Decisão Volkszählungsurteil (Deutschland, 1983) é reconhecida como o marco teórico decisivo para a reorientação conceitual da privacidade para a autodeterminação informativa. A decisão BVerfGE 65,1 (Volkszählung), proferida em 15 de dezembro de 1983 pelo Tribunal Constitucional Federal (TFC) alemão, foi seminal ao reconhecer o *Rech Auf Infomationelle Selbstbestimmung* (autodeterminação como direito informativo).

Daquele marco em diante, o conceito foi recebendo contribuições provindas tanto da jurisprudência quanto de parlamentos de países membros da Comunidade Europeia, porém o intenso comércio e circulação de mercadorias e pessoas, nesses territórios, culminou com a aprovação de uma diretiva comum, o qual se tornou outro marco jurídico fundamental para o desenvolvimento da autodeterminação informacional. Assim, a Diretiva n. 95/46/CE do Parlamento Europeu e do Conselho (de 24 de outubro de 1995) representou um avanço significativo na proteção de dados pessoais e na harmonização legislativa europeia, sendo um dos pilares da chamada quarta geração de leis de proteção

Revista | Direitos Sociais e Políticas Públicas Unifafibe

de dados (Oliveira, 2023). Seus principais pontos de destaque foram: objetivo de harmonização e livre circulação de dados; estabelecimento de princípios fundamentais; criação de autoridade de controle; e, influência global.

A RSL II também identificou as causas que tornaram a Diretiva 95/46/CE obsoleta, exigindo sua substituição pelo Regulamento Geral de Proteção de Dados - GDPR (União Europeia, 2016). Entre as causas estavam a explosão do *Big Data* e as novas formas de tratamento, as limitações do *Safe Harbor*, e a necessidade de um empoderamento efetivo do titular. Outros eventos catalizaram sua obsolescência, como o 11 de setembro[7] e as revelações de *Edward Snowden* sobre programas como *Prism* e *Upstream*.[8] Estes eventos confirmaram o Estado de Vigilância, alertando que a vigilância em massa abrange não apenas o conteúdo das comunicações, mas também os metadados.

Assim, como estratégia para enfrentar essa nova realidade de segurança, o GDPR da União Europeia foi um marco ao instrumentalizar e conferir efetividade ao conceito de autodeterminação informativa. Ele estabeleceu um modelo de proteção abrangente e transversal, reafirmando o princípio da autodeterminação informativa e enfatizando o consentimento qualificado ("livre, específico e inequívoco").

No entanto, a literatura apontou críticas e desafios relacionados ao GDPR. Dentre as críticas mais ferrenhas ao GDPR, está a que aponta para a sua elevada dependência do consentimento como exigência normativa para o tratamento de dados pessoais. Embora o Regulamento exija que ele seja “livre, específico, informado e explícito” (GDPR, art. 6º), a realidade da interação digital compromete frequentemente a validade e a real liberdade dessa manifestação de vontade (Carvalho, 2023; Costa, 2020; Gueiros, 2023; Oliveira, 2023; Ruviaro, 2021; Silva, 2017; Videira, 2022).

A literatura apontou para uma “fadiga do consentimento”, vez que os usuários, sobrecarregados pela complexidade e volume das políticas de privacidade, tendem a

[7] BBC News Brasil. ***Atentados de 11 de Setembro: a tragédia que mudou os rumos do século 21***. Disponível em: https://www.bbc.com/portuguese/internacional-55351015. Visitado em: 07.nov.2025.
[8] The Guardian. ***NSA Files Decoded: what the revelations mean for you.*** By Ewen Macaskill and Gabriel Dance. Produced by Feilding Cage and Greg Chen. Published on November 1, 2013. Disponível em: https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1. Visitado em: 07.nov.2025.

Revista | Direitos Sociais e Políticas Públicas Unifafibe

aceitá-las de forma superficial, sem plena compreensão das implicações do tratamento de seus dados (Carvalho, 2023; Costa, 2020; Silva, 2017). Essa "escolha real" é frequentemente viciada por "padrões obscuros de design" (dark patterns) que influenciam o comportamento dos titulares (Gralha, 2022, s/p), ou pela imposição de restrições de serviço caso o consentimento não seja dado, mesmo que o GDPR proíba que controladores dificultem a prestação de serviços por falta de permissão (Carvalho, 2023).

Outro ponto é a discussão quanto ao direito à explicação, considerando que a GDPR é permeada por dúvidas, e autores apontam que o excessivo enfoque em direitos individuais pode limitar a capacidade de lidar com impactos coletivos (Alimonti, 2021; Barbosa, 2022; Martins, 2021).

O debate sobre o tratamento de dados pessoais sensíveis ganha complexidade exponencial no contexto do Big Data e dos algoritmos de Inteligência Artificial, desafiando a definição formal estabelecida pela Lei Geral de Proteção de Dados (LGPD). O artigo menciona acertadamente o questionamento da ANPD quanto ao uso de dados sensíveis inferíveis para treinar IA generativa sob a base legal de Legítimo Interesse. Crucperfilização ameaça não reside apenas nos dados fornecidos explicitamente, mas na inferência algorítmica de categorias sensíveis, como filiação política, convicção religiosa ou orientação sexual. Os modelos de IA podem, a partir da análise massiva de dados não sensíveis (comportamento de navegação, padrões de compra, interações em redes sociais), deduzir com alta precisão informações que, se coletadas diretamente, seriam categorizadas como sensíveis e exigiriam cautela reforçada e consentimento específico, conforme o Art. 5º, II, da LGPD.

Além disso, há um desafio em conciliar a transparência algorítmica com o segredo comercial (Alimonti, 2021). Tal Zarsky, por exemplo, critica a incompatibilidade de certos princípios do GDPR, como a limitação de finalidade, a minimização de dados, a definição de dados sensíveis e a regulação de decisões automatizadas, com a lógica do Big Data (Martins, 2021; Zarsky, 2014).

Neste sentido, a tutela da autodeterminação informativa deve incorporar uma reavaliação de como o Direito lida com a inferência de sensibilidade. O conceito

Revista | Direitos Sociais e Políticas Públicas | Unifafibe

tradicional de dado sensível, que se baseia na declaração explícita do titular, torna-se insuficiente na era do aprendizado de máquina. A inferência cria um vácuo regulatório onde informações altamente íntimas e discriminatórias são tratadas como meros dados comportamentais, permitindo a contornabilidade das restrições impostas a bases legais mais permissivas, como o Legítimo Interesse. Portanto, aprimorar a LGPD exige estender o regime protetivo dos dados sensíveis para englobar as categorias de informações que são inferidas e utilizadas para fins de perfilização, garantindo que os algoritmos de IA não se tornem ferramentas de discriminação oculta ou de mineração não autorizada da esfera íntima do indivíduo.

3.3 Evolução histórico-normativa do direito à autodeterminação informativa no ordenamento jurídico brasileiro

O caminho de reconhecimento da autodeterminação informativa no Brasil foi um processo gradual e multifacetado, evoluindo de um amparo implícito na Constituição Federal para a consagração como direito fundamental autônomo. A trajetória perpassou microssistemas legais, decisões jurisprudenciais e culminou em uma lei geral específica e na Emenda Constitucional de 2022.

Embora o termo "autodeterminação informativa" não estivesse explicitamente na Constituição Federal de 1988 (CF/88), o ordenamento jurídico já estabelecia alicerces indiretos para a proteção de dados pessoais.

A dignidade da pessoa humana (Art. 1º, III), reconhecida como fundamento primordial da República. A capacidade de autodeterminar-se informativamente é vista como um elemento essencial para o livre desenvolvimento da personalidade e para a construção da subjetividade, sendo a dignidade humana a cláusula geral de tutela que abarca essa proteção. A privacidade e a intimidade (Art. 5º, X) atuavam como fundamentos da proteção da autodeterminação informativa antes de sua consolidação expressa. O *habeas data* (Art. 5º, LXXII) foi concebido para assegurar o conhecimento e a retificação de informações pessoais constantes em bancos de dados governamentais ou de caráter público. A jurisprudência do Supremo Tribunal Federal (STF), em particular no

Revista | Direitos Sociais e Políticas Públicas Unifafibe

RE n. 673.707/MG e na ADI 6.387/DF, foi singular ao extrair do Habeas Data não apenas uma garantia processual, mas um direito material à autodeterminação informativa.

A literatura aponta também a existências de Microssistemas legais precursores, que pavimentaram o terreno jurídico para edificação daquele instituto. O Quadro 1 demonstra as legislações e suas contribuições para a autodeterminação informativa.

Quadro 1. Microssistemas legais precursores à autodeterminação informativa

Legislação	***Ano***	***Contribuição para a autodeterminação informativa***
Lei Estadual n. 824 (Rio de Janeiro)	1984	Foi o primeiro texto normativo no Brasil a tutelar o direito à autodeterminação informativa, alinhando-se aos debates europeus da época
Código de Defesa do Consumidor (CDC) (Lei n. 8.078)	1990	Desempenhou um papel pioneiro ao estabelecer o dever de informação, a transparência e o direito de acesso e correção de dados nas relações de consumo
Lei do Cadastro Positivo (LCP) (Lei n. 12.414)	2011	Embora focada em informações públicas (publicidade como regra), fortaleceu a transparência estatal e fomentou a emergência de um sujeito informacional ativo que busca o controle das informações, complementando a tutela do Habeas Data.
Marco Civil da Internet (MCI) (Lei n. 12.965)	2014	Foi o primeiro diploma legal a abordar explicitamente a proteção da privacidade no ambiente digital. Estabeleceu princípios como consentimento (embora principiológico), inviolabilidade das comunicações e o direito à exclusão definitiva de dados pessoais ao término da relação (Art. 7º, X). Contudo, reconheceu a necessidade de uma lei específica posterior para a efetivação completa da proteção de dados.

A plena autonomização e o reconhecimento da autodeterminação informativa vieram com a legislação específica e a reforma constitucional:

A Lei Geral de Proteção de Dados (LGPD) (Lei n. 13.709) (2018) emergiu como o marco regulatório fundamental no Brasil, consagrando explicitamente a autodeterminação informativa como um de seus fundamentos (Art. 2º, II). A lei instrumentaliza esse direito por meio de um catálogo granular de direitos do titular (como acesso, retificação, anonimização, portabilidade e revisão de decisões automatizadas) e qualifica o consentimento como "manifestação livre, informada e inequívoca". A criação da Autoridade Nacional de Proteção de Dados (ANPD) também é uma contribuição estratégica, atuando como a terceira linha de defesa (administrativa).

Revista | Direitos Sociais e Políticas Públicas Unifafibe

A Emenda Constitucional n. 115/2022 elevou a proteção de dados pessoais a um patamar constitucional explícito, conferindo-lhe a natureza de direito e garantia fundamental autônoma. Ao ser inserida no Art. 5º da CF/88, a proteção de dados adquiriu o status de cláusula pétrea. Essa mudança reforça a autoridade da LGPD e consolida formalmente o entendimento de que a proteção de dados, alicerçada na autodeterminação informativa, é essencial para o livre desenvolvimento da personalidade na era digital.

Em síntese, o reconhecimento da autodeterminação informativa no Brasil passou de uma proteção difusa e setorial (tutelada pelo *Habeas Data* e pelo CDC) para uma proteção sistêmica e fundamental, focada no controle do indivíduo sobre seu corpo eletrônico.

O subtítulo a seguir registras os resultados obtidos a partir de estudos de caso sobre procedimentos de fiscalização realizados pela ANPD e DPC em redes sociais; especialmente sobre o Caso Schrems II (UNIÃO EUROPEIA. Tribunal de Justiça da União Europeia, 2020) e o Caso Google Spain (Costeja), (UNIÃO EUROPEIA. Tribunal de Justiça da União Europeia, 2014).

4. AUTODETERMINAÇÃO INFORMATIVA E REDES SOCIAIS: VIOLAÇÕES NO BASIL E NA IRLANDA

Esta seção está dividida em duas subseções, a primeira sintetiza as causas de violação a autodeterminação informativa em redes sociais extraídas dos procedimentos de fiscalização conduzidos pela ANPD, abrangendo as Notas Técnicas (BTs) n. 1, n. 2, n. 3 e n. 4 e n. 5, que investigam as práticas das redes sociais. A segunda, os eventos obtidos a partir das decisões proferidas pela *Data Protection Commission* (DPC) da Irlanda.

4.1 Causas de violação à autodeterminação informativa por redes sociais fiscalizadas pela ANPD

Note-se, o estandarte da autodeterminação informativa atua, tanto ativa ou passivamente, em ação ou reação, ou omissão, do indivíduo em controlar o tráfego e a quem seja um destinatário em potencial, e mais, não só a destinação, mas como se faz e

Revista | Direitos Sociais e Políticas Públicas Unifafibe

em que extensão se tem à utilização desses dados sensíveis pessoais. As decisões da ANPD mostram que esse controle é frequentemente minado pelas práticas das plataformas.

O Quadro 2 evidencia que a falta de transparência é uma causa recorrente, impedindo que o usuário exerça seu controle ativo por meio de decisões informadas.

Quadro 2. Causas de Violações Relacionadas à Transparência e Informação:

Causa de Violação	Detalhes e Exemplos (ANPD)	NTs Relacionadas
Finalidades Genéricas e Opacas	A ANPD criticou finalidades de tratamento como "para informar os algoritmos da Plataforma" (TikTok) ou "fornecer e aprimorar nossos Produtos" (Meta). Tais menções foram consideradas insuficientemente precisas para cobrir o processamento massivo de dados (ex: para treinar IA generativa), configurando um uso secundário dos dados sem o devido conhecimento dos titulares.	NT n. 2, n. 3, n. 4
Assimetria de Informação	No caso da Meta e da IA generativa, a ANPD constatou que a comunicação sobre a alteração da política de privacidade foi insuficiente, não sendo clara, ampla ou em boa-fé. Foi observado que a Meta agiu com menos transparência no Brasil do que na União Europeia (onde houve notificação por e-mail e in-app)	NT n. 3, n. 4
Inconsistência e Obstrução	O TikTok foi criticado por apresentar respostas genéricas, inconclusivas e até inverídicas, dificultando a avaliação técnica e sinalizando uma insuficiência de colaboração esperada de um agente regulado	NT n. 5
Falta de Correlação	O WhatsApp, em sua política inicial, não correlacionava claramente as bases legais às finalidades e categorias de dados pessoais tratados para titulares brasileiros, dificultando a transparência.	NT n. 1

O Quadro 3 demonstra que o tratamento de dados sem uma base legal válida ou que excede as legítimas expectativas é um ponto central de fiscalização.

Revista | Direitos Sociais e Políticas Públicas Unifafibe

Quadro 3. Causas Relacionadas à Ilegalidade do Tratamento (Bases Legais)

Causa de Violação	Detalhes e Exemplos (ANPD)	NTs Relacionadas
Uso Ilegítimo de Legítimo Interesse (IA Generativa)	A ANPD questionou veementemente o uso do "legítimo interesse" (Art. 7º, IX) pela Meta para treinar sistemas de IA generativa. A Autoridade enfaticamente declarou que o tratamento de dados pessoais sensíveis (inferíveis a partir de fotos e vídeos) não pode ser fundamentado no legítimo interesse.	NT n. 3, n. 4
Uso Inadequado de Execução de Contrato (Menores)	No caso do TikTok, a ANPD questionou o uso da base legal de "execução de contrato" para o tratamento de dados de crianças e adolescentes. A Autoridade destacou que menores de 16 anos são absolutamente incapazes de celebrar contratos válidos, tornando o tratamento de dados com base nessa premissa fundamentalmente ilegal.	NT n. 2, n. 5
Violação das Legítimas Expectativas	A falta de especificidade nas finalidades frustra as expectativas legítimas dos usuários e configura uma interferência indevida no direito à autodeterminação informativa do titular.	NT n. 4

O Quadro 4 aponta que a ANPD focou significativamente na proteção de crianças e adolescentes e na falha das plataformas em garantir a segurança dos dados.

Quadro 4. Causas Relacionadas à Proteção de Vulneráveis e Segurança

Causa de Violação	Detalhes e Exemplos (ANPD)	NTs Relacionadas
Inadequação da Proteção de Crianças	O TikTok foi criticado por mecanismos de verificação de idade insuficientes e ineficazes (uso de "Age Gate" por autodeclaração) que permitem o cadastro indevido de milhões de crianças.	NT n. 2, n. 5
"Feed Sem Cadastro" (TikTok)	A ANPD identificou o recurso "feed sem cadastro" como um problema regulatório grave, permitindo o tratamento de dados em larga escala de crianças e adolescentes e o perfilamento de usuários não registrados sem uma base legal válida. A ANPD determinou a suspensão imediata desse recurso no Brasil devido ao risco de dano grave.	NT n. 5
Salvaguardas para IA Generativa (Menores)	Não foram inicialmente identificadas salvaguardas adequadas para o tratamento de dados de menores de 18 anos para fins de treinamento de IA generativa. A Meta se comprometeu a não incluir dados publicamente disponíveis de contas brasileiras menores de 18 anos no treinamento de IA generativa "neste momento"	NT n. 4
Privacy by Design/Default Deficiente	A ANPD ressaltou que, embora o WhatsApp ofereça mecanismos de privacidade, muitas funcionalidades (como “visto por último” ou autenticação em duas etapas) são opcionais e não habilitadas por padrão, divergindo do ideal de "privacidade por padrão" (onde a configuração mais privada é a default)	NT n. 1

Revista | Direitos Sociais e Políticas Públicas Unifafibe

O Quadro 5 destaca como as plataformas dificultam o exercício do direito de oposição (opt-out), essencial para o controle reativo do titular.

Quadro 5. Causas Relacionadas ao Exercício dos Direitos (Controle Reativo)

Causa de Violação	Detalhes e Exemplos (ANPD)	NTs Relacionadas
Mecanismo de Opt-out Obscuro	No caso do uso de dados para IA generativa pela Meta, o mecanismo de opt-out (direito de oposição) foi considerado obscuro e de difícil compreensão, dificultando a manifestação de contrariedade dos usuários	NT n. 3, n. 4
Ônus Excessivo para Não-usuários	A ANPD identificou que o formulário de oposição impunha dificuldades e ônus excessivos aos não-usuários (pessoas que não possuem conta). A Meta foi obrigada a simplificar o formulário, removendo campos obrigatórios desnecessários	NT n. 4
Dificuldade de Acesso	Foi solicitada a disponibilização em destaque das informações para o titular exercer seus direitos na primeira camada da Política de Privacidade do WhatsApp, a fim de simplificar o acesso	NT n. 1

A análise das Notas Técnicas demonstra que a ANPD utiliza uma abordagem de regulação responsiva, priorizando medidas orientativas e preventivas, mas adotando medidas mais enérgicas, como a suspensão de tratamento (medida preventiva), quando há risco iminente de dano grave e irreparável ou ilegalidade flagrante no tratamento de dados (como o uso de dados de crianças ou o treinamento de IA com dados sensíveis via legítimo interesse).

O esforço regulatório visa combater a assimetria de poder e informação que transforma o exercício da autodeterminação informativa em uma "mera ficção jurídica", exigindo das plataformas não apenas o cumprimento formal da LGPD, mas uma readequação de seus modelos de negócio.

Na seção seguinte, apresenta-se os Estudos de Caso de decisões proferidas pela Data Protection Commission (DPC) da Irlanda.

Revista | Direitos Sociais e Políticas Públicas Unifafibe

4.2 Causas de violação à autodeterminação informativa por redes sociais fiscalizadas pela *Data Protection Commission* (DPC) da Irlanda.

A DPC atua como autoridade supervisora principal (*Lead Supervisory Authority* - LSA) para as operações transfronteiriças de grandes empresas de tecnologia (*Big Techs*) na União Europeia, incluindo o Grupo Meta (*WhatsApp, Facebook e Instagram*), devido à sua sede europeia na Irlanda. As decisões da DPC demonstram violações sistêmicas ao direito fundamental à autodeterminação informativa (o poder ativo e reativo do indivíduo de controlar seus dados), geralmente pela falha em cumprir os requisitos do Regulamento Geral sobre a Proteção de Dados (GDPR).

A DPC identificou que as plataformas falharam reiteradamente em fornecer informações claras e acessíveis, tornando o consentimento e o controle individual uma "mera ficção jurídica", o Quadro 6 registra como isso ocorreu em cada caso.

Quadro 6. Falta de Informação e Transparência Inadequada

Caso DPC	Natureza da Violação	Detalhes da DPC e Impacto
DPC n. 1 (WhatsApp)	Opacidade para Não-usuários	O WhatsApp falhou totalmente em cumprir as obrigações de transparência (Art. 14 GDPR) para não-usuários, cujos números de telefone eram considerados dados pessoais. A falha na transparência foi classificada como infração ao princípio fundamental de transparência (Art. 5(1)(a) GDPR) e de gravidade muito séria
DPC n. 4 & 5 (Facebook/Instagram)	Informação Confusa e Desarticulada	O Facebook/Instagram não forneceu informações claras e concisas sobre as operações de tratamento de dados, finalidades e bases legais. A informação estava desligada e generalizada, exigindo que os usuários "trabalhassem muito" para entender as operações, o que lhes impedia de exercer seus direitos de forma significativa
DPC n. 2 (Instagram/Crianças)	Informação Incompreensível para Vulneráveis	Houve falha na clareza e acessibilidade das informações sobre o processamento de dados, o que é agravado pelo fato de crianças estarem menos cientes dos riscos, consequências e salvaguardas envolvidas.

Revista | Direitos Sociais e Políticas Públicas Unifafibe

A DPC, sob a direção vinculativa do *European Data Protection Board* (EDPB), refutou as bases legais usadas pela Meta para justificar seu modelo de negócio, o Quadro 7 registra a Inadequação das Bases legais e Violações ao Princípio da Lealdade:

Quadro 7. Inadequação das Bases Legais e Violação do Princípio da Lealdade

Caso DPC	Natureza da Violação	Detalhes da DPC e Impacto
DPC n. 4 & 5 (Facebook/Instagram)	Execução de Contrato (Art. 6º(1)(b) GDPR)	A Meta fundamentou sua defesa no fato de que a publicidade comportamental se justifica para a execução serviço já contratado. O EDPB/DPC refutou, determinando que a publicidade personalizada não é objetivamente necessária para o propósito principal do Facebook/Instagram (comunicação e conexão). O modelo de negócio deve adaptar-se ao RGPD, e não o contrário.
DPC n. 4 & 5 (Facebook/Instagram)	Violação do Princípio da Lealdade (*Fairness*)	O serviço foi apresentado de forma enganosa, e a situação de "pegar ou largar" (*take-it-or-leave-it*) imposta aos usuários, juntamente com a assimetria de informações, violou o princípio da lealdade (Art. 5º(1)(a)). O princípio da lealdade visa corrigir a assimetria de poder entre controladores e titulares de dados.
DPC n. 6 (Transferências para os EUA)	Ilegalidade da Transferência Internacional	As transferências de dados da Meta *Ireland* para os EUA eram ilegais (Art. 46(1) GDPR) porque a legislação dos EUA (como o Setor 702 da FISA e a EO 12333) não garante um nível de proteção essencialmente equivalente ao da EU.

A DPC também demonstrou rigor na aplicação dos princípios de *Privacy by Design* e *Privacy by Default*, bem como na proteção de dados sensíveis e de segurança. O Quadro 8 identifica as falhas na segurança, *privacy by design* e proteção de vulneráveis.

Revista | Direitos Sociais e Políticas Públicas Unifafibe

Quadro 8. Falhas na Segurança, Privacy by Design e Proteção de Vulneráveis

Caso DPC	Natureza da Violação	Detalhes da DPC e Impacto
DPC n. 3 (*Facebook/Scraping*)	*Privacy by Design/Default* Violado (Art. 25)	A Meta infringiu os princípios de Proteção de Dados desde a Concepção e por Defeito. A configuração padrão permitia que números de telefone e *e-mails* fossem acessíveis via "pesquisa inversa", expondo dados de 533 milhões de usuários globalmente ao *scraping* (coleta automatizada.
DPC n. 2 (Instagram/Crianças)	Exposição de Menores e Alto Risco	A configuração "pública por padrão" para contas de crianças e a publicação obrigatória de informações de contato representavam um risco elevado. Isso expôs os menores ao risco de raspagem de dados e comunicação com indivíduos perigosos (assédio, abuso, tráfico).
DPC n. 7 (*Facebook*/Senhas)	Falhas Críticas de Segurança	Armazenamento inadvertido de senhas em texto simples (*plaintext*) nos sistemas internos do *Facebook Lite*, afetando dezenas de milhões de usuários. Isso foi uma falha grave e sistêmica na implementação de medidas de segurança.

As falhas regulatórias tiveram o impacto direto de limitar a capacidade do usuário de exercer o controle reativo sobre seus dados. As Autoridades (ANPD e DPC) têm consistentemente punido a ausência de mecanismos de *Privacy by Design e Privacy by Default*, reafirmando a necessidade de que a proteção de dados seja incorporada desde a concepção do sistema e permaneça como padrão (default), conforme idealizado originalmente por Cavoukian (2011). O Quadro 9 registra os obstáculos ao exercício dos direitos e dano imediato aos titulares.

Revista | Direitos Sociais e Políticas Públicas Unifafibe

Quadro 9. Obstáculos ao Exercício dos Direitos e Dano Imediato aos Titulares

Caso DPC	Natureza da Violação	Detalhes da DPC e Impacto
DPC n. 4 & 5 (*Facebook/Instagram*)	"Pegar ou Largar"	A imposição de termos de serviço sob uma situação de "tudo ou nada" ou "pegar ou largar" limitou o controle e privou os usuários de direitos importantes
DPC n. 6 (Transferências para os EUA)	Ausência de Recurso Judicial Efetivo	A lei dos EUA (FISA 702/EO 12333) não confere aos titulares de dados da UE direitos acionáveis perante os tribunais dos EUA contra as autoridades americanas. Essa falha viola a essência do direito fundamental a um recurso judicial efetivo (Art. 47 da Carta)
DPC n. 7 (*Facebook*/Senhas)	Falha de Notificação	A Meta falhou em notificar a violação de senhas dentro de 72 horas (Art. 33(1) GDPR), o que impediu a DPC de exercer seus poderes regulatórios para proteger os titulares em tempo hábil.
DPC n. 3 (*Facebook/Scraping*)	Risco de Fraude e Roubo de Identidade	O *scraping* expôs usuários a riscos severos de fraude, roubo de identidade, falsificação e ataques de *phishing* ou *smishing*, além da perda de controle.

A DPC adota uma postura regulatória assertiva e utiliza o modelo de supervisão principal (*Lead Supervisory Authority - LSA*) do GDPR, o Quadro 10 descreve como a Autoridade Irlandesa aplicou suas estratégias de fiscalização.

Quadro 10. Estratégias de Fiscalização da DPC

Estratégias de fiscalização	Aplicações
Poderes Corretivos Abrangentes	A DPC aplica multas administrativas substanciais. Os valores são calculados com base no faturamento mundial anual da "empresa" (*undertaking*), e não apenas da subsidiária irlandesa, resultando em multas de até €1,2 bilhão (DPC n. 6 - Transferências de Dados)
Ordem de Conformidade e Repreensão	Emite repreensões formais e ordens de conformidade com prazos definidos (e.g., 3 meses) para que a empresa regularize o processamento
Colaboração Vinculativa (EDPB)	A DPC consulta o EDPB (Comitê Europeu para a Proteção de Dados), que emite direções vinculativas que a DPC deve seguir. Essa colaboração garante a aplicação consistente do GDPR em toda a União Europeia
Suspensão de Tratamento	A DPC ordenou a suspensão das transferências de dados da Meta Ireland para a Meta US e exigiu a cessação do tratamento e armazenamento ilegal de dados nos EUA, estabelecendo que o modelo de negócio deve se adaptar à conformidade.
Monitoramento Continuado	O monitoramento é garantido por meio de prazos específicos para implementação e pela exigência de relatórios de conformidade

Revista | Direitos Sociais e Políticas Públicas Unifafibe

A DPC opera como o supervisor de alfândega digital da União Europeia. Seu trabalho não se resume a verificar se os rótulos (políticas de privacidade) estão escritos corretamente. Ela verifica a qualidade intrínseca do produto (o tratamento de dados), questionando se os "ingredientes" (bases legais) são legítimos e se a segurança dos contêineres (sistemas de *Privacy by Design/Default*) é forte o suficiente contra roubos (*scraping*) e acidentes (senhas em texto simples). Acima de tudo, a DPC fiscaliza se a "porta de entrada" (transferência de dados para os EUA) tem um nível de segurança equivalente, garantindo que a soberania digital europeia não seja comprometida e que o cidadão não perca o direito de buscar justiça.

5. INTERSECÇÕES ENTRE DECISÕES BRASILEIRA E IRLANDESA

Os Estudos de caso identificaram as interseções entre as decisões brasileiras e as decisões análogas proferidas no âmbito da Autoridade Irlandesa de Proteção de Dados (DPC-Irlanda) proferidas em face das mesmas redes sociais investigadas nos procedimentos brasileiros. Os quadros a seguir resumem os achados de pesquisa sobre o que ambas as autoridades investigaram.

5.1 Problema regulatório

O problema regulatório central comum é a falha sistêmica das plataformas em garantir o controle ativo e reativo do titular sobre seus dados.

Quadro 12. Problema Regulatório (Interseção na Causa da Violação)

Problema regulatório	Intersecção na causa da violação
Violação dos Princípios Fundamentais (Legalidade, Lealdade e Transparência)	Constatou-se que as infrações sistêmicas comprometem princípios basilares de ambas as leis (GDPR/LGPD)
Assimetria de Poder e Informação	Ambas atuam para corrigir o desequilíbrio, que faz com que o autocontrole individual (consentimento ou direito de saída) seja insuficiente para garantir a proteção de direitos da personalidade

Revista | Direitos Sociais e Políticas Públicas Unifafibe

5.2 Análise de políticas regulatórias

As políticas de tratamento das plataformas foram rejeitadas por ambas as autoridades devido às falhas descritas no Quadro 13.

Quadro 13. Análise de Políticas Regulatórias (Interseção nas Bases Legais e Princípios)

Causa de Violação Comum	Detalhe da Convergência (ANPD e DPC)
Falta de Transparência	Ambas identificaram que as políticas de privacidade eram "insuficientes e confusas" (DPC, 2021) ou "dispersas e sem a especificação necessária" (ANPD, 2022). Essa falta de clareza impede que os usuários compreendam quais dados são compartilhados, para quais finalidades e com que base legal, comprometendo sua capacidade de tomar decisões informadas.
Bases Legais Inadequadas	O uso do contrato como base legal foi refutado em ambos os contextos: a DPC/EDPB determinou que a publicidade comportamental não é "objetivamente necessária" para a execução do contrato do serviço principal da Meta. A ANPD, por sua vez, questionou a "execução de contrato" para o tratamento de dados de menores no *TikTok*, devido à incapacidade legal de menores de 16 anos celebrarem contratos válidos.
Legítimo Interesse Genérico	Ambas as autoridades levantaram preocupações sobre o uso do "legítimo interesse" para finalidades "demasiadamente genéricas". A ANPD pacificou que o tratamento de dados pessoais, especialmente os sensíveis (partindo de fotos ou vídeos para IA generativa), não pode ser fundamentado no legítimo interesse.
Privacy by Design/Default	Ambas criticaram falhas sistemáticas das plataformas em implementar medidas técnicas e organizacionais apropriadas. A DPC apontou a configuração "pública por padrão" do Instagram para contas de crianças. A ANPD notou que muitas funcionalidades de privacidade do *WhatsApp* são "opcionais e não habilitadas por padrão", divergindo do ideal de privacidade por padrão.
Proteção de Vulneráveis	Ambas reconheceram a hipervulnerabilidade de crianças e adolescentes e criticaram a ineficácia dos mecanismos de verificação de idade (como o uso de "*Age Gate*" por autodeclaração) e a ausência de salvaguardas específicas para esse público
Obstáculos ao Exercício de Direitos	Ambas constataram que a falta de informação clara e a imposição de uma "situação de pegar ou largar" (aceitar os termos ou ser excluído do serviço) impedem o exercício efetivo do controle reativo (como o direito de oposição). A ANPD criticou o mecanismo de *opt-out* da Meta para IA generativa por ser "obscuro e de difícil compreensão".

5.3 Análise de impactos

Os impactos identificados nas diferentes jurisdições são convergentemente graves, conforme demonstrado no Quadro 14:

Revista | Direitos Sociais e Políticas Públicas Unifafibe

Quadro 14. Análise de Impactos (Interseção nas Consequências)

Impacto Comum	Detalhe da Convergência (ANPD e DPC)
Perda de Control	O impacto central é a privação da capacidade dos usuários de exercerem a autodeterminação informativa, pois não conseguem tomar decisões informadas sobre seus dados pessoais.
Riscos de Dano Grave	Ambas as autoridades apontam riscos concretos decorrentes das violações. A DPC apontou riscos de fraude, roubo de identidade e *spamming* por *scraping*. A ANPD identificou o risco de dano grave e irreparável no uso de dados para treinamento de IA generativa, com potencial para criação de *deepfakes* e uso secundário irregular de dados.
Violação de Expectativas	A falta de especificidade nas finalidades do tratamento frustra as expectativas legítimas dos usuários, configurando uma interferência indevida no direito à autodeterminação informativa.

5.4 Estratégias de fiscalização, implementação e monitoramento

No Quadro 15 registra-se que ambas as autoridades adotam uma postura regulatória assertiva, utilizando um conjunto comum de ferramentas de *enforcement*.

Quadro 15. Estratégias de Fiscalização, Implementação e Monitoramento (Interseção na Ação Regulatória)

Estratégia	Interseção na Ação Regulatória
Início dos Inquéritos	As investigações são iniciadas tanto por iniciativa própria (*own-volition inquiry*) quanto por reclamações de titulares de dados.
Adoção de Medidas Corretivas Padrão	Ambas emitem repreensões formais e ordens de conformidade (exigindo que as empresas corrijam o tratamento de dados e forneçam informações claras).
Sanções Dissuasórias	As duas autoridades impõem multas administrativas substanciais calculadas com base em fatores como a natureza, gravidade e duração da infração, o número de titulares afetados e o grau de negligência.
Posicionamento Comum:	Ambas compartilham o entendimento de que o "modelo de negócio deve adaptar-se aos requisitos do RGPD/LGPD, e não o contrário"

Em suma, a convergência entre ANPD e DPC confirma que as grandes plataformas de tecnologia enfrentam os mesmos desafios regulatórios globais no que diz respeito à transparência, legalidade e proteção de usuários vulneráveis. A atuação coordenada e convergente das autoridades é vista como o único mecanismo eficaz contra a assimetria de poder exercida pelas *Big Techs*, reafirmando que o direito à autodeterminação informativa assume uma dimensão coletiva/garantista.

Revista | Direitos Sociais e Políticas Públicas Unifafibe

6. APRIMORANDO A PROTEÇÃO DA AUTODETERMINAÇÃO INFORMATIVA: PROPOSIÇÃO DE MELHORIAS

As propostas de melhoria buscam fortalecer a LGPD e o sistema regulatório brasileiro, atuando em três frentes: aprimoramento legislativo (substancial), fortalecimento dos mecanismos de controle (processual) e consolidação da infraestrutura institucional (estratégica).

6.1 Aprimoramento legislativo e regulamentação específica

O consenso entre os estudos revisados é a necessidade de desenvolver um marco legal mais robusto, atualizado e específico para a relação entre usuários e plataformas digitais.

Quadro 16. Aprimoramento Legislativo e Regulamentação Específica

Aprimoramento	Justificativa
Legislação Especial para Redes Sociais	É necessária a criação de legislação especial (além da LGPD) que discipline a relação entre o usuário e a rede social, dadas as complexidades e os riscos inerentes a esse modelo de negócio.
Melhoria da Regulamentação de Cookies	A LGPD deve ser atualizada para tornar a política de cookies mais robusta, especialmente quando comparada ao regime europeu (GDPR), onde a regulamentação é mais detalhada.
Direito Penal e Cooperação Internacional	É sugerida a necessidade de alinhamento das legislações nacionais com as internacionais e o aprimoramento da legislação penal, com a definição de penalidades específicas e tipificações claras para o tráfico de dados pessoais
Limites ao Uso Secundário de Dados	A ANPD deve promover maior rigor na fiscalização do uso secundário de dados, exigindo clareza e transparência para coibir a prática irregular.
Legislação sobre Comportamentos Digitais	É proposta a discussão sobre aprimoramento da legislação para incriminar práticas associadas ao cancelamento virtual.

6.2 Fortalecimento da transparência e do consentimento qualificado

Visto que o consentimento é frequentemente uma "mera ficção jurídica" devido à assimetria informacional, as propostas descritas no Quadro 17, levantadas a partir das revisões sistemáticas de literatura aplicadas na tese, visam resgatar a autonomia do titular.

Revista | Direitos Sociais e Políticas Públicas Unifafibe

Quadro 17. Fortalecimento da Transparência e do Consentimento Qualificado

Aprimoramento	Justificativa
Transparência e Boa-fé	É fundamental que a ANPD exija transparência na gestão do fluxo informacional. O tratamento de dados deve ser claro e preciso.
Mecanismos Alternativos ao Consentimento (Nudges)	Devem ser explorados mecanismos ou abordagens que reforcem a proteção do indivíduo além do consentimento. O uso de *privacy nudges* (incentivos sutis) é sugerido como ferramenta para auxiliar o usuário a tomar decisões mais conscientes e seguras sobre a privacidade online.
Auditoria de Algoritmos	Deve-se implementar a auditoria nos algoritmos utilizados para garantir que não sejam discriminatórios ou prejudiciais ao livre desenvolvimento da personalidade.
Modelos de Negócio Responsáveis	Propõe-se investigar novos modelos de negócio que respeitem integralmente a privacidade e a autodeterminação informativa, explorando alternativas à atual economia da vigilância digital

6.3 Implementação de design e proteção de vulneráveis

As propostas visam obrigar as empresas a integrarem a proteção de dados desde a concepção de seus serviços, focando na proteção de grupos hipervulneráveis.

Quadro 18. Implementação de Design e Proteção de Vulneráveis

Aprimoramento	Justificativa
Privacy by Design/Default (PbD/PbD)	As plataformas devem ser obrigadas a adotar a proteção de dados desde a concepção e por defeito, alterando as configurações padrão para serem mais restritivas. A privacidade ideal exige que o usuário não precise tomar providências adicionais para proteger seus dados, com funcionalidades mais privadas desabilitadas por padrão.
Proteção de Crianças e Adolescente	É inadiável o desenvolvimento de diretrizes normativas mais claras para proteger a privacidade e a autodeterminação informativa de crianças. As plataformas devem implementar mecanismos mais eficazes de verificação de idade (em vez de um controle reativo a posteriori) para impedir o cadastro indevido de menores de 13 anos

6.4 Fortalecimento institucional e estratégias da ANPD

A efetividade da proteção da autodeterminação informativa depende do dirigismo informacional exercido pela ANPD, a terceira linha de defesa.

Revista | Direitos Sociais e Políticas Públicas Unifafibe

Quadro 19. Fortalecimento Institucional e Estratégias da ANPD

Aprimoramento	Justificativa
Reforço Institucional	As plataformas devem ser obrigadas a adotar a proteção de dados desde a concepção e por defeito, alterando as configurações padrão para serem mais restritivas. A privacidade ideal exige que o usuário não precise tomar providências adicionais para proteger seus dados, com funcionalidades mais privadas desabilitadas por padrão.
Educação e Conscientização	A ANPD deve promover a educação e a conscientização da população sobre seus direitos, visto que a lei por si só não garante a compreensão e o exercício pleno da autodeterminação informativa.
Aperfeiçoamento Regulatório Contínuo	Deve ser promovido o aperfeiçoamento contínuo de técnicas regulatórias, incluindo o uso de *Soft Law* para detalhar a implementação prática das normas e de *Sandbox* Regulatório para testar inovações em privacidade.
Tutela Coletiva/Garantista	A proteção do direito à autodeterminação informativa deve ser reclassificada ou tutelada pela via coletiva/garantista, pois as falhas de tratamento de dados por redes sociais são inerentemente danos transindividuais e coletivos, impossibilitando a tutela individual, como demonstrado nos casos de treinamento de IA generativa e feed sem cadastro de terceiros não-usuários.

Por fim, muitos dos problemas regulatórios e sociais críticos aqui identificados, que se concentram na erosão da autodeterminação informativa e na assimetria de poder nas redes sociais, podem ser enfrentados ou mitigados por meio de dispositivos previstos no Projeto de Lei nº 2630/2020.[9] Embora a tese se concentre na aplicação da Lei Geral de Proteção de Dados (LGPD) e do GDPR, e o PL-2630/2020 foque primariamente na integridade informacional e na responsabilidade das plataformas, as áreas de intervenção se sobrepõem significativamente, visando corrigir a opacidade e o abuso de poder que fragilizam os direitos dos usuários.

CONCLUSÃO

As investigações da Autoridade Nacional de Proteção de Dados (ANPD) demonstraram consistentemente que a dimensão individual do direito à autodeterminação informativa – manifestada pela capacidade do usuário de controlar

[9] Câmara dos Deputados. Projeto de Lei nº 2630/2020. Link: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2256735 . Acesso em: 06.11.2024.

Revista | Direitos Sociais e Políticas Públicas Unifafibe

seus dados por meio do consentimento informado ou da oposição individual – é destituída de efetividade nas práticas de tratamento de dados pelas redes sociais.

Isso ocorre porque as empresas frequentemente agem ignorando o consentimento (como no tratamento de dados de terceiros não garantista, garantindo que a fiscalização e o poder sancionatório obter adesões, o que compromete a autonomia do titular.

Consequentemente, a proteção desse direito fundamental passa por uma transmutação na prática regulatória: a autodeterminação informativa transcende sua natureza como apenas um direito da personalidade para exigir, prioritariamente, uma tutela coletiva e garantista (Kuner, 2013; Didier Jr., Zaneti Jr., 2021).

Nesse cenário, a atuação da ANPD, enquanto terceira linha de defesa administrativa, consolida-se como o único mecanismo eficaz para confrontar a assimetria de poder exercida pelas *big techs*.

Em conclusão, a tutela efetiva da autodeterminação informativa no ambiente digital depende, portanto, da consolidação dessa dimensão garantista, garantindo que a fiscalização e o poder sancionatório da Autoridade prevaleçam sobre a lógica da exploração informacional, reafirmando a dignidade da pessoa humana.

REFERÊNCIAS

ALIMONTI, Veridiana. Algoritmos e autodeterminação: uma contribuição a partir das noções de autodeterminação informativa e controle no contexto de decisões automatizadas. Tese de Doutorado. São Paulo: Faculdade de Direito, Universidade de São Paulo, 2021. Orientador: Prof. Dr. Vinícius Marques de Carvalho. Disponível em: https://repositorio.usp.br/item/003211614. Acesso em: 12 mai. 2025.

BARBOSA, Tales Schmidke. O direito à explicação nas decisões automatizadas: uma análise à luz do devido processo informacional e do sistema jurídico brasileiro. Porto Alegre, 2022. Dissertação (Mestrado em Direito)– Programa de Pós-Graduação em Direito, Escola de Direito, Pontifícia Universidade Católica do Rio Grande do Sul, Porto Alegre, 2022. Orientadora: Dra. Regina Linden Ruaro. Disponível em: https://tede2.pucrs.br/tede2/handle/tede/10294. Acesso em/. 12 mai. 2025.

Revista | Direitos Sociais e Políticas Públicas Unifafibe

BRANCO, S. (Org.); TEFFÉ, Chiara Spadaccini de (Org.); FERNANDES, E. R. (Org.). Privacidade e proteção de dados de crianças e adolescentes. 1. ed. Rio de Janeiro: ITS Rio, 2024. v. 1. 298p.

BRASIL, Superior Tribunal de Justiça. Recurso Especial n. -34.498/SP. Recorrente: Carlos Alberto Brilhante Ustra. Min. Relatora: Nancy Andrighi. Brasília, DF, 5 fev. 2015. Disponível em: https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=201304162180&dt_publicacao=05/02/2015. Acesso 3 jul. 2025

BRASIL. Constituição da República Federativa do Brasil de 1988. Brasília: Diário Oficial da União, seção 1, 5 out. 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 19 jan. 2025.

BRASIL. Lei n. 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Diário Oficial da União: seção 1, Brasília, DF, 24 abr. 2014, p. 1. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 11 abr. 2025.

BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Diário Oficial da União: seção 1, Brasília, DF, ano 155, n. 157, p. 59-64, 15 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 15 ago. 2025.

BRASIL. Receita Federal. Cartilha para utilização do Centro Virtual de Atendimento ao Contribuinte – e-CAC. Brasília: Receita Federal do Brasil, [s.d.]. Disponível em: https://www.conjur.com.br/dl/ca/cartilha-receita-fed1.pdf . Acesso em: 13 ago. 2025.

BRASIL. Secretaria de Governo Digital (SGD). Guia de elaboração de inventário de dados pessoais. Brasília: Ministério da Gestão e da Inovação em Serviços Públicos, 2021. Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_inventario_dados_pessoais.pdf. Acesso em: 01 mar. 2025.

BRASIL. Superior Tribunal de Justiça. AgInt no REsp n. -93.873/SP. Recorrente: Google Brasil Internet Ltda. Recorrido: S. M. S. Relatora: Min. Nancy Andrighi, 3. Turma, julgado em 19 mar. 2018. Diário de Justiça Eletrônico, Brasília, DF, 19 mar. 2024.

BRASIL. Superior Tribunal de Justiça. Recurso Especial -16.921/RJ. Relatora Ministra Nancy Andrigui. Recorrente: Google Brasil Internet Ltda. Recorrida: Maria da Graça Xuxa Meneghel, decisão de 26.06.2012, Dje. Diário de Justiça Eletrônico, Brasília, DF, 26 jun. 2025.

Revista | Direitos Sociais e Políticas Públicas | Unifafibe

BRASIL. Superior Tribunal de Justiça. Recurso Especial n. -40.721/GO. Ministro Relator Maria Isabel Gallotti. Brasília, 11 out. 2016. Disponível em: https://ww2.stj.jus.br/processo/revista/inteiroteor/?num_registro=201400501100&dt_publicacao=11/11/2016. Acesso em: 13 fev. 2025.

BRASIL. Superior Tribunal de Justiça. Recurso Especial n. 1.626.739/RS. Ministro Relator: Luis Felipe Salomão. Brasília, 09 maio 2017. Disponível em: https://ww2.stj.jus.br/processo/revista/documento/mediado/?componente=ATC&sequencial=74184067&num_registro=201602455869&data=20170801&tipo=5&formato=PDF. Acesso em: 17 fev. 2025.

BRASIL. Superior Tribunal de Justiça. Recurso Especial n. 22.337/RS. Recorrente: Clube de Diretores Logistas de Passo Fundo-RS. Relator: Rui Rosado de Aguiar. Brasília, DF, 13 fev. 1995. Diário da Justiça da República Federativa do Brasil, Brasília, DF, 20 mar. 1995.

BRASIL. Superior Tribunal de Justiça. Recurso Especial n. 957.343/DF. Ministro Relator Aldir Passarinho Jr. Brasília, 18 mar. 2008. Disponível em: https://ww2.stj.jus.br/processo/revista/inteiroteor/?num_registro=201400501100&dt_publicacao=11/11/2016. Acesso em: 13 fev. 2025.

BRASIL. Supremo Tribunal Federal. Ação Direta de Inconstitucionalidade n. 4.815. Requerente: Associação Nacional dos Editores de Livros. Relator: Ministra Carmen Lúcia. Brasília, 10 jun. 2015. Disponível em: http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=10162709. Acesso em: 31 maio 2025.

BRASIL. Supremo Tribunal Federal. Ação Direta de Inconstitucionalidade n. 6.387 MC-REF/DF. Rel. Ministra Rosa Weber, julgado 07/05/2020. Diário de Justiça Eletrônico, Brasília, DF, 12 nov. 2020. Disponível em: https://portal.stf.jus.br/processos/downloadPeca.asp?id=15344949214&ext=.pdf. Acesso em: 10 out. 2024.

BRASIL. Supremo Tribunal Federal. Ação Direta de Inconstitucionalidade n. 6.397. Relator: Ministro Luís Roberto Barroso. Julgado em: 22 fev. 2023. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/stf/1772808221/inteiro-teor-1772808224. Acesso em: 08 jul. 2025.

BRASIL. Supremo Tribunal Federal. Medida cautelar na ação direta de inconstitucionalidade 6.561/Tocantis. Rel. Min. Luiz Edson Fachin. Julg. 13 out. 2020. Disponível em: https://redir.stf.jus.br/estfvisualizador-pub/jsp/consultarprocessoeletronico/ConsultarProcessoEletronico.jsf?seqobjetoincidente=6008887. Acesso em: 08 nov. 2024.

Revista | Direitos Sociais e Políticas Públicas Unifafibe

BRASIL. Supremo Tribunal Federal. Pena pode ser cumprida após decisão de segunda instância, decide STF. Supremo Tribunal Federal, Brasília/DF, 17 fev. 2016. Disponível em: http://www.stf.jus.br/portal/cms/verNoticiaDetalhe.asp?idConteudo=310153&caixaBusca=N. Acesso em: 19 ago. 2025.

BRASIL. Tribunal Superior do Trabalho. Embargos em Recurso de Revista. Processo E-RR-933-49.2012.5.10.0001. Rel. Min. Maria Helena Mallmann. Órgão Judicante: Subseção I Especializada em Dissídios Individuais. Julgamento em 16 dez. 2021. Publicação do acórdão: 25 fev. 2022. Disponível em: https://consultaprocessual.tst.jus.br/consultaProcessual/consultaTstNumUnica.do?consulta=Consultar&conscsjt=&numeroTst=933&digitoTst=49&anoTst=2012&orgaoTst=5&tribunalTst=10&varaTst=0001&submit=Consultar. Acesso em: 27 fev. 2025.

CARVALHO, Cesar Augusto Rodrigues de. Autodeterminação informativa e sociedade de controle. 2023. 343 f. Tese (Doutorado)– Universidade de São Paulo, São Paulo, 2023. Orientadora: Profa. Dra. Elza Pereira Cunha Boiteux. Disponível em: https://repositorio.usp.br/item/003159018. Acesso em: 12 mai. 2025.

CAVOUKIAN, Ann. Privacy by Design: The 7 Foundational Principles. Toronto: Office of the Information and Privacy Commissioner of Ontario, 2011.

COSTA, Ramon Silva. Entre taps e direitos: proteção de dados pessoais, privacidade e liberdade no aplicativo Grindr. 2020. 185 f. Dissertação (Mestrado em Direito)– Universidade Federal de Juiz de Fora, Faculdade de Direito, Juiz de Fora, 2020. Orientador: Prof. Dr. Sergio Marcos Carvalho de Ávila Negri. Disponível em: https://repositorio.ufjf.br/jspui/bitstream/ufjf/12068/1/ramonsilvacosta.pdf. Acesso em: 23 mar. 2025.

DATA PROTECTION COMMISSION (DPC). Decision IN-18-5-7: Meta Platforms Ireland Ltd. – Children's Data Processing Inquiry. Dublin: DPC, 31 dez. 2022d. Disponível em: https://www.dataprotection.ie/sites/default/files/uploads/2022-12/2022_3-2_Decision_IN-18-5-7_Childrens_(Reclamation).pdf. Acesso em: 14 jul. 2025.

DATA PROTECTION COMMISSION (DPC). Decision IN-20-8-1: Meta Platforms Ireland Ltd. – Data Transfers Inquiry. Dublin: DPC, 5 dez. 2023. Disponível em: https://www.dataprotection.ie/sites/default/files/uploads/2023-12/2023_12.05_Decision_IN-20-8-1_Meta%20Platform%20Ireland%20Limited%20(Facebook)%20data%20transfers.pdf. Acesso em: 14 jul. 2025.

Revista | Direitos Sociais e Políticas Públicas Unifafibe

DATA PROTECTION COMMISSION (DPC). Decision IN-21-4-2: Meta Platforms Ireland Ltd. (formerly Facebook Ireland Ltd). Dublin: DPC, 25 nov. 2022b. Disponível em: https://www.dataprotection.ie. Acesso em: 14 jul. 2025.

DATA PROTECTION COMMISSION (DPC). Decision on the Inquiry into Instagram Ireland Ltd under Section 110 of the Data Protection Act 2018 and Article 65 of the GDPR. Dublin: DPC, 2 set. 2022. Disponível em: https://www.dataprotection.ie/sites/default/files/uploads/2022-09/2022_02.09_Decision_IN%2009-09-22_Instagram.pdf. Acesso em: 14 jul. 2025.

DATA PROTECTION COMMISSION (DPC). Decision on the Inquiry into Meta Platforms Ireland Ltd. (formerly Facebook Ireland Ltd.) under Section 110 of the Data Protection Act 2018 and Article 65 of the GDPR. Dublin: DPC, 31 dez. 2022c. Disponível em: https://www.dataprotection.ie/sites/default/files/uploads/2022-12/2022_3-2_DECISION%20(ADOPTED)Meta(Facebook).pdf. Acesso em: 14 jul. 2025.

DATA PROTECTION COMMISSION (DPC). Decision on the Inquiry into WhatsApp Ireland Ltd under Section 110 of the Data Protection Act 2018 and Article 65 of the GDPR. Dublin: DPC, 20 ago. 2021. Disponível em: https://www.dataprotection.ie/sites/default/files/uploads/2021-09/2021_20.08_Decision_Full_WhatsApp_Ireland.pdf. Acesso em: 14 jul. 2025.

DATA PROTECTION COMMISSION (DPC). Final Decision IN-19-4-1: Meta Platforms Ireland Ltd. – Redacted Version. Dublin: DPC, 26 set. 2024. Disponível em: https://www.dataprotection.ie/sites/default/files/uploads/2024-09/2024_26.09_Meta-Final-Decision-IN-19-4-1-Redacted.pdf. Acesso em: 14 jul. 2025.

DATA PROTECTION COMMISSION. One Stop Shop (OSS). Dublin: DPC, [s.d.]. Disponível em: https://www.dataprotection.ie/en/organisations/international-transfers/one-stop-shop-oss. Acesso em: 13 ago. 2025.

DEUTSCHLAND. Bundesverfassungsgericht. BVerfGE 34, 238 – Tonband. 2 BvR 454/71. Beschluss vom 31. Januar 1973. In: Entscheidungen des Bundesverfassungsgerichts. Karlsruhe: Bundesverfassungsgericht, 1973. Disponível em: https://www.servat.unibe.ch/dfr/bv034238.html. Acesso em: 23 mar. 2025.

DEUTSCHLAND. Bundesverfassungsgericht. BVerfGE 65, 1 – Volkszählung. 1 BvR 209/83, 1 BvR 484/83, 1 BvR 440/83, 1 BvR 420/83, 1 BvR 362/83, 1 BvR 269/83. Alemanha, 15 de dezembro de 1983. Disponível em: http:// www.servat.unibe.ch/dfr/bv065001.html. Acesso em: 19 junho 2025.

DIDIER JR., Fredie; ZANETI JR., Hermes. Direito Processual Civil: Processo Coletivo. 15. ed. Salvador: Editora JusPodivm, 2021.

Revista | Direitos Sociais e Políticas Públicas | Unifafibe

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

EUROPEAN COMISSION. Decision on Meta's GDPR Violation. Case No. 2023. Bruxelles: EDPB, 2023. Disponível em: https://www.edpb.europa.eu/our-work-tools/our-documents/binding-decision-board-art-65/binding-decision-12023-dispute-submitted_en. Acesso em 4 abr. 2025.

EUROPEAN COMISSION. Guidelines 4/2018 on Transparency. Bruxelles: EDPB, 2018. Disponível em: https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42018-accreditation-certification-bodies-under_en. Acesso 4 abr. 2025.

EUROPEAN COMISSION. Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679. Brussels: Directorate General Justice, 2017. 22 p. Disponível em: https://ec.europa.eu/newsroom/article29/items/611236. Acesso em: 11 jul. 2025.

EUROPEAN COMISSION. Guidelines on the Territorial Scope of the GDPR. Bruxelles: EDPB, 2019. Disponível em: https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en_1.pdf. Acesso em: 4 abr. 2025.

EUROPEAN COMISSION. Proposal for a Regulation on Artificial Intelligence. 2021. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021PC0206. Acesso 4 abr. 2025.

EUROPEAN COMMISSION. Ethics Guidelines for Trustworthy AI. 2019. Disponível em: https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai. Acesso e: 4 abr. 2025.

EUROPEAN DATA PROTECTION BOARD. Regulamento interno: versão 8. Bruxelas, EDPB, 2022. Disponível em: https://www.edpb.europa.eu/our-work-tools/our-documents/rules-procedure/rules-procedure-version-8_en. Acesso em: 11 jul. 2025.

GRALHA, Patrícia Maria Meireles. Os limites materiais do consentimento dos titulares de dados no comércio eletrônico: uma análise crítica das políticas de privacidade dos 30 (trinta) maiores varejistas/marketplaces em número de acessos do Brasil em 2022. 2022. 106 f. Dissertação (Mestrado em Direito da Regulação)– Escola de Direito do Rio de Janeiro, Fundação Getúlio Vargas, Rio de Janeiro, 2022. Orientador: Prof. Dr. Luca Belli. Disponível em: https://repositorio.fgv.br/items/46e3f3b0-e6c7-4625-97d2-f440c53ce96d. Acesso em: 12 mai. 2025.

Revista | Direitos Sociais e Políticas Públicas Unifafibe

GUEIROS, Pedro Teixeira. O consentimento do titular de dados nas relações online: parâmetros para a validade e o exercício do controle informacional. 2023. Dissertação (Mestrado em Direito)– Pontifícia Universidade Católica do Rio de Janeiro, Rio de Janeiro, 2023. Disponível em: https://www.maxwell.vrac.pucrio.br/colecao.php?msg=28. Acesso em 13 mar. 2025.

JUSTEN FILHO, Marçal. Curso de Direito Administrativo. 15. ed. São Paulo: Revista dos Tribunais, 2020.

KUNER, Christopher. European Data Privacy Law: Reform and Regulation of the European Data Economy. Oxford: Oxford University Press, 2013.

MARTINS, Pedro Bastos Lobo. A regulação do profiling na Lei Geral de Proteção de Dados: o livre desenvolvimento da personalidade em face da governamentalidade algorítmica. 2021. 195 f. Dissertação (Mestrado em Direito) Universidade Federal de Minas Gerais, Faculdade de Direito, Belo Horizonte, 2021. Orientador: Prof. Dr. Brunello Stancioli. Disponível https://repositorio.ufmg.br/handle/1843/43900. Acesso em: 12 mai. 2025.

OLIVEIRA, Rodrigo de Souza; COSTA, Mariana Ferreira. Funções de hash e sua aplicação na segurança da informação: uma abordagem técnica e jurídica. Revista Brasileira de Direito da Tecnologia da Informação, v. 4, n. 2, p. 115–132, 2023. Disponível em: https://seer.ufrgs.br/index.php/rbdti/article/view/12987. Acesso em: 12 jul. 2025.

RUVIARO, Eduardo Missau. (Des) Proteção de dados e internet das coisas: os desafios à tutela dos dados de saúde de usuários de dispositivos de IoT à luz dos preceitos da LGPD. 2021. 129 f. Dissertação (Mestrado em Direito)– Programa de Pós-Graduação em Direito, Universidade Federal de Santa Maria (UFSM), Santa Maria, RS, 2021. Orientador: Prof. Dr. Rafael Santos de Oliveira. Disponível em: https://repositorio.ufsm.br/handle/1/23085. Acesso em: 12 mai. 2025.

SILVA, Alexandre Ribeiro da. A proteção de dados no Brasil: a tutela do direito à privacidade na sociedade de informação. 2017. Dissertação (Mestrado em Direito e Inovação)– Programa de Pós-Graduação Stricto Sensu da Faculdade de Direito, Universidade Federal de Juiz de Fora, Juiz de Fora, 2017. Orientador: Prof.ª Dra. Lucia Maria Paschoal Guimarães. Disponível: https://repositorio.ufjf.br/jspui/bitstream/ufjf/5374/1/alexandreribeirodasilva.pdf. Acesso em: 12 mai. 2025.

SOARES, Marcelo Negri; KAUFFMAN, Marcos Eduardo; CHAO, Kuo-Ming; SAAD, Omar Saad. New Technologies and the Impact on Personality Rights in Brazil. Pensar - Revista de Ciências Jurídicas, v. 25, p. 1-12, 2020. Disponível: https://ojs.unifor.br/rpen/article/view/9969. Acesso em: 12 mai. 2025.

Revista | Direitos Sociais e Políticas Públicas Unifafibe

TEPEDINO, Gustavo; PEREIRA, Rodrigo da Cunha. Desafios da Responsabilidade Civil Contemporânea. São Paulo: Editora OAB-SP ESA, 2024.

UNIÃO EUROPEIA. Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995. Relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Jornal Oficial da União Europeia, 23 nov. 1995. Disponível em: http://eur-lex.europa.eu/legal-content/pt/TXT/?uri=CELEX%3A31995L0046. Acesso em: 30 jul. 2025.

UNIÃO EUROPEIA. Parlamento Europeu; Conselho da União Europeia; Comissão Europeia. Carta dos Direitos Fundamentais da União Europeia. Bruxelas: União Europeia, 2000. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:12016P/TXT. Acesso em: 29 jul. 2025.

UNIÃO EUROPEIA. Parlamento Europeu; Conselho da União Europeia. Regulamento (UE) 2016/679, de 27 de abril de 2016. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016R0679. Acesso em: 08 jul. 2025.

UNIÃO EUROPEIA. Tribunal de Justiça da União Europeia. Processo C-131/12 – Google Spain SL e Google Inc. v. Agencia Española de Protección de Datos (AEPD) e Mario Costeja González. Julgado em: 13 maio 2014. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131. Acesso em: 08 jul. 2025.

UNIÃO EUROPEIA. Tribunal de Justiça da União Europeia. Processo C-362/14 – Maximillian Schrems v. Data Protection Commissioner. Julgado em: 6 out. 2015. Disponível em: https://curia.europa.eu. Acesso em: 08 jul. 2025.

UNIÃO EUROPEIA. Tribunal de Justiça da União Europeia. Caso Schrems II. Decisão C-311/18. 2020. Disponível em: https://www.edpb.europa.eu/news/news/2020/european-data-protection-board-publishes-faq-document-cjeu-judgment-c-31118-schrems_pt. Acesso em: 4 abr. 2025.

VIDEIRA, Yuri Araújo Primo. A mitigação da privacidade na era dos dispositivos eletrônicos de captação de voz frente ao consentimento e a autodeterminação informativa. 2022. 106 f. Dissertação (Mestrado em Direito)– Programa de PósGraduação em Direito, Pontifícia Universidade Católica de Minas Gerais, Belo Horizonte, 2022. Orientador: Prof.ª Dra. Lígia Dabul. Disponível em: https://bib.pucminas.br/autoridades?q=28157&for=AUTORIDADE_TODOS&aut_id=28157. Acesso em: 12 mai. 2025.

Revista | Direitos Sociais e Políticas Públicas Unifafibe

WARREN, Samuel; BRANDEIS, Louis. The Right to Privacy. Harvard Law Review, v. 4, n. 5, p. 193-220, 1890.

ZARSKY, Tal. Understanding discrimination in the scored society. Washington Law Review, Washington, v. 89, n. 4, p. 1375–1412, 2014. Disponível em: https://digitalcommons.law.uw.edu/wlr/vol89/iss4/10/. Acesso em: 29 jul. 2025.