

**Hipervulnerabilidade No Ambiente Digital:
Perspectivas Jurídicas, Sociais E Educacionais Na Era Da IA**

Jamara Cardoso Neves Braz¹

Katia Cristian Puente Muniz²

Claudia Helena dos Santos Araújo³

RESUMO

Este artigo analisa a hipervulnerabilidade no ambiente digital a partir de uma abordagem interdisciplinar que articula direito, sociologia clínica e educação. A pesquisa, de natureza qualitativa e bibliográfica, discute como condições históricas, culturais e econômicas amplificam a exposição de grupos estruturalmente vulneráveis, como crianças, mulheres, idosos e pessoas com deficiência, a riscos digitais, como exclusão, discriminação algorítmica e violência simbólica. Do ponto de vista jurídico, examina a evolução normativa e jurisprudencial sobre proteção de dados e governança digital no Brasil, incluindo a Constituição Federal, o Marco Civil da Internet, a LGPD e o recém-promulgado ECA Digital (Lei 15.211/2025). A perspectiva sociológico-psicanalítica interpreta o mal-estar contemporâneo como produto da visibilidade excessiva, da pressão algorítmica e da fragilidade das mediações simbólicas. Já o eixo educacional destaca a importância da alfabetização digital crítica e de políticas públicas de inclusão como estratégias de prevenção e fortalecimento da cidadania. O artigo conclui que a efetiva proteção da hipervulnerabilidade digital requer integração entre direito, educação e políticas públicas de governança algorítmica.

¹ Advogada e pedagoga. Presidente da Comissão de Direito Educacional da OAB/RJ e da Associação Brasileira de Direito Educacional Seccional Rio de Janeiro. Docente FAETEC. Mestre em Educação/Políticas Públicas (UNESA, 2023) e pós-graduada em Direito Educacional, Docência no Ensino Superior em Direito (UNIFOA/OAB-RJ). Orcid: <https://orcid.org/0000-0002-7979-168X> . jamarabraz@yahoo.com.br

² Socióloga clínica. Doutora em Psicanálise e Sociedade, UVA-RJ. Mestre em Sociologia pela UFRJ. Docente no Doutorado em Psicanálise, Saúde e Sociedade na Universidade Veiga de Almeida. Conselheira Científica da ABT. Pesquisadora Fundación Esplai-Espanha. katia.muniz@uva.br . Orcid <https://orcid.org/0000-0002-6998-7021>

³ ³ Doutora em Educação. Pós-doutora em Estudos Culturais (UFRJ). Associada à ANPEd. Sócia da SBPC. Pesquisadora ABT, Cátedra de Educação Básica Alfredo Bosi (IEA-USP) e Educa+AI, Educação e Inteligência Artificial. Docente no Mestrado em Educação do IFG e de Educação Profissional e Tecnológica (ProfEPT). helena.claudia@ifg.edu.br

PALAVRAS-CHAVE: Proteção de dados pessoais. Cidadania digital. Educação digital. Governança algorítmica. Hipervulnerabilidade digital.

1. INTRODUÇÃO

A noção de vulnerabilidade tem ocupado espaço crescente nos debates contemporâneos, especialmente diante da centralidade das plataformas digitais na vida social. Se antes era compreendida como fragilidade individual, hoje emerge o conceito de hipervulnerabilidade, que evidencia como condições históricas, econômicas e culturais produzem sujeitos expostos a riscos acentuados. Crianças, mulheres, idosos e pessoas com deficiência constituem grupos que, já marcados por vulnerabilidades estruturais, encontram no ambiente digital a amplificação de exclusões, riscos e violências simbólicas.

O Brasil representa um contexto singular para essa discussão, combinando ampla conectividade, desigualdades sociais persistentes e fragilidade na regulação das plataformas. Ao mesmo tempo, o país participa de um debate global sobre governança digital, direitos fundamentais e cidadania online.

Este artigo propõe uma leitura interdisciplinar da hipervulnerabilidade digital, articulando perspectivas jurídicas, sociológicas, psicanalíticas e educacionais. A questão central que orienta o estudo é: de que maneira a hipervulnerabilidade de crianças, idosos, mulheres e pessoas com deficiência se manifesta nas plataformas digitais, e quais estratégias jurídicas, sociais e educacionais podem promover sua proteção efetiva?

A investigação adota abordagem qualitativa e bibliográfica, baseada em produções acadêmicas publicadas entre 2019 e 2025, relatórios institucionais e documentos oficiais. O recorte metodológico abrange estudos sobre hipervulnerabilidade digital com destaque para análises sobre visibilidade algorítmica, exclusão digital e mal-estar contemporâneo.

No campo jurídico, são considerados marcos como a Constituição Federal, o Marco Civil da Internet, a Lei Geral de Proteção de Dados (LGPD), o Estatuto da Criança e do Adolescente e o Estatuto do Idoso, além de jurisprudências recentes. A metodologia integra análise documental normativa e revisão crítica da literatura, em perspectiva interdisciplinar, para compreender como os dados, algoritmos e políticas digitais impactam a cidadania e os direitos fundamentais na sociedade em rede.

2. MARCOS LEGAIS E DESAFIOS DA PROTEÇÃO DIGITAL

2.1. Marcos legais: Constituição, Marco Civil da Internet, LGPD, Estatuto da Criança e do Adolescente e Estatuto do Idoso.

Muito se debate hoje em dia sobre a insegurança digital em que vivemos a partir da explosão do uso de tecnologias após a pandemia de COVID-19 e o isolamento social. Com a ascensão das plataformas digitais e da inteligência artificial (IA) conjugada com opacidade dos algoritmos, novos desafios aos direitos fundamentais, sobretudo no tocante à privacidade, à intimidade e à não discriminação, emergem exigindo uma regulação e proteção dos usuários buscando minimizar a hipervulnerabilidade.

No âmbito das políticas públicas, observa-se que há instrumentos disponíveis para regulamentação. No entanto, alcançar uma governança efetiva exige mais do que avanços normativos: requer a implementação de medidas práticas sustentadas por uma abordagem multissetorial que envolva governo, judiciário, empresas e o Congresso Nacional buscando promover um incentivo mais consistente à educação digital.

Nosso quadro normativo brasileiro é robusto na tentativa de proteção, no entanto, com o avanço do uso de tecnologias e considerando as inúmeras denúncias e acontecimentos em nossa sociedade, novos marcos regulatórios são necessários, como se verifica na própria jurisprudência. Ele é composto pela Constituição Federal, o Marco Civil da Internet, a Lei Geral de Proteção de Dados (LGPD), o Estatuto da Criança e do Adolescente (ECA) e o Estatuto do Idoso que oferece a base jurídica da proteção digital, mas revela limites frente à lógica algorítmica e à economia de dados.

2.2. A Constituição Federal (1988) e a LGPD – Emenda Constitucional nº 115/2022

A Constituição Federal de 1988 garante, em seu art. 5º, incisos X e XII, o direito à intimidade, à honra, à vida privada e à inviolabilidade das comunicações. Nos arts. 205, 227 e 230 consagram o direito à educação e a proteção especial à criança, ao adolescente e ao idoso, estabelecendo o fundamento ético-jurídico da cidadania digital.

A Emenda Constitucional nº 115/2022 incluiu expressamente a proteção de dados pessoais entre os direitos e garantias fundamentais, reconhecendo-a como autônoma e essencial à dignidade humana. Em sintonia, a Lei Geral de Proteção de Dados (Lei nº 13.709/2018) representou um avanço substancial ao disciplinar o tratamento de dados sensíveis, especialmente de grupos vulneráveis, e ao instituir a Autoridade Nacional de Proteção de Dados (ANPD). Inspirada no

Regulamento Europeu (GDPR), a LGPD estabelece princípios como finalidade, necessidade, transparência e segurança, assegurando ao titular o direito de acesso, retificação e eliminação de informações.

O Supremo Tribunal Federal consolidou entendimento de que a proteção de dados é condição para o exercício da liberdade individual e para a preservação da democracia informacional. No RE 1.306.208/DF (Tema 1.046), reconheceu a autonomia e fundamentalidade do direito à proteção de dados; na ADI 6.387/DF, declarou a inconstitucionalidade da MP 954/2020, ao considerar desproporcional o compartilhamento de dados de usuários de telefonia com o IBGE. Já no RE 1.344.771/SP (Tema 1.189), afirmou que a proteção de dados deve ser interpretada como extensão do direito à privacidade, inclusive no setor público. Tais precedentes evidenciam que, embora a Constituição fundamente o regime de proteção digital, o Estado ainda carece de instrumentos de governança algorítmica e controle democrático das tecnologias emergentes.

No contexto recente, falhas de segurança em instituições públicas, como a Secretaria de Educação do Distrito Federal, a Unicamp e o Instituto de Pesquisas Energéticas e Nucleares (Ipen), revelam a hipervulnerabilidade digital das estruturas educacionais e científicas brasileiras.

Em perspectiva internacional, a OCDE (2020) defende que o uso da inteligência artificial deve servir a valores humanos, com políticas de IA confiável, voltadas à transparência, à segurança e à prevenção de vieses discriminatórios. No mesmo sentido, o STJ, no REsp 1.940.150/SP, reconheceu que o uso indevido de dados pessoais configura dano moral *in re ipsa*, reforçando a responsabilidade civil pelo tratamento irregular de informações.

Por sua vez, o TSE, nas eleições de 2022, identificou que o microdirecionamento algorítmico e o impulsionamento segmentado podem ferir o princípio da isonomia entre candidatos, exigindo maior transparência na publicidade digital. Esses julgados demonstram que, embora a LGPD represente marco essencial, ainda são necessárias normas complementares específicas para a IA e o perfilamento comportamental, capazes de garantir efetiva proteção de direitos fundamentais na era algorítmica.

2.3. Marco Civil da Internet (Lei nº 12.965/2014)

O Marco Civil da Internet - reconhecido pelo STF como o *estatuto da liberdade na rede* - institui princípios de neutralidade de rede, liberdade de expressão, proteção à privacidade e

responsabilização de provedores. Em RE 1.037.396/SC (Tema 533)⁴, o STF reinterpreta o Marco Civil da Internet, a medida em que estabelece que as plataformas devem atuar proativamente contra conteúdos ilícitos específicos, como os que envolvem pornografia infantil e terrorismo, pornografia infantil, induzimento ao suicídio, tráfico de pessoas, golpes de Estado e ainda devem remover conteúdos ofensivos à honra e à imagem de pessoas após notificação, se atentando que sua obrigação de monitoramento ativo para evitar a proliferação desses atos sob pena de responsabilidade civil pressupondo uma falha sistêmica.

Além disso, o Tema determina o acatamento dos seguintes pontos: 1. que o provedor de internet poderá ser responsabilizado civilmente se, após ordem judicial específica, não remover conteúdo ilícito, consagrando o modelo de *responsabilidade subsidiária condicionada*. Esse entendimento garante a liberdade de expressão, mas também evidencia um ponto crítico: o poder concentrado das plataformas em moderar e priorizar conteúdo sem transparência; 2. com a finalidade de proteger os usuários de internet e responsabilizar empresas que hospedem conteúdo online obriga-as a removerem publicações ofensivas sem a necessidade de uma ordem judicial, ou seja, que assuma o controle do que é hospedado em suas empresas ou seja, dever de fiscalizar; 3. exige que as plataformas devem ter sede e representante legal no Brasil com poderes para responder judicial e administrativamente, prestar informações às autoridades e cumprir determinações judiciais

Com essa decisão denota-se que o Marco Civil da Internet se mostra insuficiente para lidar com sistemas algorítmicos opacos, mineração de dados e personalização de conteúdo, fenômenos inexistentes à época de sua promulgação. Assim, sua eficácia depende de interpretação conforme a LGPD e a Constituição, de modo a incorporar deveres de transparência algorítmica e mitigação de vieses automatizados.

2.4. ECA - Estatuto da Criança e do Adolescente (Lei nº 8.069/1990) e o Estatuto do Idoso (Lei nº 10.741/2003)

O Estatuto da Criança e do Adolescente (ECA) consagra o princípio da proteção integral (arts. 1º e 4º), impondo deveres de prevenção e salvaguarda diante das novas formas de violação de direitos na esfera digital. Crianças e adolescentes, como sujeitos em desenvolvimento, exigem

⁴ Em Tema 533 - Dever de empresa hospedeira de sítio na internet fiscalizar o conteúdo publicado e de retirá-lo do ar quando considerado ofensivo, sem intervenção do Judiciário. Disponível em: <https://portal.stf.jus.br/jurisprudenciarepercussao/veramentoprocesso.asp?incidente=5217273&numeroprocesso=1057258&classeprocesso=re&numerotema=533>

garantias reforçadas frente à exposição indevida, ao *cyberbullying*, ao marketing direcionado e ao uso indevido de dados sensíveis.

Em conjunto, o Estatuto do Idoso (Lei nº 10.741/2003) amplia a noção de proteção integral, estendendo-a à prevenção da exclusão digital e à proteção contra fraudes e desinformação. Apesar do arcabouço normativo, a educação digital insuficiente permanece um obstáculo: a legislação prevê proteção, mas não assegura a formação crítica dos usuários. A judicialização excessiva da proteção digital reflete a ausência de políticas públicas preventivas e de governança integrada.

A OCDE (2020) observa que a aplicação da inteligência artificial na educação e em ambientes digitais impõe novos desafios de confiança, transparência e responsabilidade. Essa diretriz reforça a necessidade de articular legislação, regulação técnica e alfabetização digital para uma proteção humanizada e efetiva.

A jurisprudência tem ampliado a compreensão da hipervulnerabilidade digital. No REsp 1.783.269/MG, o Superior Tribunal de Justiça reconheceu a prevalência do ECA como norma protetiva especialíssima, considerando que a omissão das plataformas configura violação do dever de proteção integral. Já o Tribunal Superior Eleitoral, no Recurso Ordinário Eleitoral nº 0603975-98 (Caso Francischini), cassou mandato parlamentar por disseminação de *fake news*, afirmando que a desinformação digital ameaça a integridade democrática e o direito coletivo à informação verdadeira.

Nesse contexto surge a Lei nº 15.211/2025, conhecida como ECA Digital, ou Estatuto Digital da Criança e do Adolescente, que representa um avanço normativo significativo. A nova lei amplia a proteção integral ao ambiente virtual e estabelece diretrizes para redes sociais, jogos eletrônicos, aplicativos, lojas de apps e plataformas digitais. Seus principais fundamentos incluem: o interesse superior da criança como parâmetro central; a exigência de verificação confiável de idade e controle parental acessível; a proibição de monetização ou impulsionamento de conteúdos erotizados envolvendo menores; a remoção imediata de conteúdos que violem direitos, independentemente de ordem judicial; e sanções que incluem multas, suspensão ou proibição de atividades das plataformas infratoras.

O ECA Digital também atribui competências à Anatel para encaminhar ordens de suspensão de conteúdos e prevê cooperação interinstitucional entre ANPD, Ministério Público e Conselhos Tutelares. Contudo, a implementação da lei suscita dilemas éticos e técnicos, como o risco de

tecnologias intrusivas (biometria e reconhecimento facial) e potenciais conflitos com a LGPD, o Marco Civil da Internet e o próprio ECA de 1990, especialmente quanto à compatibilização entre remoção imediata de conteúdo, contraditório e liberdade de expressão. Esses desafios revelam a necessidade de uma governança ético-jurídica da infância digital, capaz de equilibrar proteção, privacidade e autonomia progressiva. Órgãos como a ANPD, o Ministério Público e os Conselhos Tutelares enfrentam, porém, restrições estruturais diante da opacidade algorítmica das plataformas, que dificulta a responsabilização efetiva. Como destaca a OCDE (2020, p. 15), “a confiança só é possível quando há transparência e explicabilidade nos critérios e algoritmos”.

Em síntese, o ECA Digital inaugura uma nova fase de proteção da infância na era algorítmica, ao integrar princípios da LGPD, do Marco Civil da Internet e do ECA original em um mesmo regime protetivo. O desafio, contudo, está em transformar essa legislação inovadora em mecanismos operacionais de fiscalização, educação e responsabilização, capazes de garantir que a inovação tecnológica avance com base na dignidade humana e nos direitos fundamentais.

Inúmeras são as decisões nos nossos Tribunais, somente para exemplificar que, de 17 jurisprudências, todas elas versam sobre hipervulnerabilidade de idosos com as fraudes de empréstimos

0802760-43.2022.8.19.0023 - APELAÇÃO Des(a). DENISE LEVY TREDLER - Julgamento: 23/09/2025 - SÉTIMA CÂMARA DE DIREITO PRIVADO (ANTIGA 12ª CÂMARA CÍVEL) APELAÇÃO CÍVEL. RELAÇÃO DE CONSUMO. AÇÃO DECLARATÓRIA DE INEXISTÊNCIA DE NEGÓCIO JURÍDICO. INDENIZAÇÃO POR DANOS MATERIAIS E MORAIS. EMPRÉSTIMO CONSIGNADO. CONTRATAÇÃO ELETRÔNICA. CONSUMIDOR HIPERVULNERÁVEL. PESSOA IDOSA E ANALFABETA. FRAUDE POR CORRESPONDENTE BANCÁRIO. RESPONSABILIDADE OBJETIVA DA INSTITUIÇÃO FINANCEIRA. NULIDADE DO NEGÓCIO JURÍDICO. 1. A relação jurídica entre instituição financeira e tomador de empréstimo consignado configura relação de consumo, aplicando-se as disposições do Código de Defesa do Consumidor. 2. A condição de pessoa idosa e analfabeta caracteriza *hipervulnerabilidade* nas relações de consumo, a exigir da instituição financeira cautelas ainda

maiores na verificação da efetiva e consciente manifestação de vontade. 3. Embora a legislação reconheça a validade dos contratos eletrônicos e assinaturas *digitais* (Lei nº 14.063/2020 e art. 225 do CC), a mera existência de procedimentos tecnológicos de autenticação não afasta a possibilidade de fraude, especialmente em se tratando de consumidor hipervulnerável. 4. As instituições financeiras respondem objetivamente por fraudes praticadas por terceiros no âmbito de operações bancárias, caracterizando-se como fortuito interno (Súmula 479/STJ). A atuação de correspondentes bancários insere-se no risco da atividade desenvolvida pela instituição financeira. 5. Incumbe à instituição financeira comprovar de forma inequívoca a regularidade da contratação e a efetiva manifestação de vontade do consumidor, especialmente quando se trata de pessoa idosa e analfabeta. 6. Caracterizada a falha na prestação do serviço bancário pela ausência de comprovação da efetiva participação consciente da consumidora no processo de contratação, impõe-se o reconhecimento da nulidade do negócio jurídico. 7. A restituição em dobro dos valores indevidamente descontados encontra fundamento no parágrafo único do art. 42 do CDC, com compensação do valor efetivamente creditado para evitar enriquecimento sem causa. 8. Os descontos indevidos em benefício previdenciário de pessoa idosa, verba de caráter alimentar, configuram dano moral *in re ipsa*. Quantum indenizatório fixado em R\$ 10.000,00 (dez mil reais) atende aos princípios da razoabilidade e proporcionalidade. 9. Aplicação das disposições da Lei nº 14.905/2024, que alterou os arts. 389 e 406 do Código Civil, estabelecendo nova sistemática baseada na diferença entre taxa SELIC e IPCA. 10. Recurso a que se nega provimento.

2.5. Casos e jurisprudências recentes envolvendo proteção digital de grupos vulneráveis

Nos últimos anos, tem se intensificado o debate sobre a responsabilidade das plataformas digitais diante de conteúdos que violam direitos humanos, especialmente de grupos vulneráveis. A seguir, destacam-se alguns casos emblemáticos e decisões recentes que ilustram avanços e desafios na proteção jurídica no ambiente virtual.

Um primeiro exemplo diz respeito ao crescimento expressivo dos crimes de misoginia online, que, entre 2017 e 2022, se tornaram a prática de ódio que mais avançou nas redes sociais brasileiras. Diante desse cenário, o Governo Federal tem adotado medidas voltadas à proteção das mulheres contra violências digitais frequentemente disfarçadas sob o discurso de liberdade de expressão. Nessa direção, o Supremo Tribunal Federal (STF) decidiu que as empresas responsáveis por redes sociais podem ser responsabilizadas pela não remoção de conteúdos que configurem crimes graves como racismo e homofobia, reconhecendo, parcialmente, a inconstitucionalidade do artigo 19 do Marco Civil da Internet (2014).

No campo da proteção à infância e adolescência, o Superior Tribunal de Justiça (STJ) reafirmou o dever das plataformas digitais de retirar conteúdos ofensivos sem necessidade de ordem judicial quando notificadas sobre publicações que violem direitos de crianças e adolescentes. A decisão surgiu a partir de um recurso envolvendo o Facebook, que se recusou a excluir uma postagem com acusações falsas e exposição indevida de um menor, consolidando o entendimento de que o princípio da proteção integral deve prevalecer nas interações digitais.

Outro dado relevante refere-se à aplicação da Lei 14.811/2024, que tipificou as práticas de *bullying* e *cyberbullying* no Código Penal. Segundo levantamento do Colégio Notarial do Brasil (CNB), divulgado pela Folha de S. Paulo e pelo Instituto Brasileiro de Direito de Família (IBDFAM), houve um aumento de 14% nas atas notariais destinadas à comprovação de casos de cyberbullying entre 2023 e 2024, alcançando mais de 145 mil registros. O crescimento revela não apenas a maior conscientização sobre os crimes virtuais, mas também o aumento das ocorrências, o que demanda políticas públicas de prevenção e educação digital.

Por fim, destaca-se a recente atuação da Justiça Eleitoral, que, nas resoluções das Eleições 2024, regulamentou o uso da inteligência artificial (IA) na propaganda política, proibindo *deepfakes* e obrigando a sinalização explícita sobre o uso da tecnologia. O Tribunal Superior Eleitoral (TSE), sob a presidência do ministro Alexandre de Moraes, também determinou a responsabilização das plataformas que não removerem, de forma imediata, conteúdos de desinformação, discursos de ódio ou manifestações de cunho antidemocrático, racista e homofóbico (TSE, 2024).

Em conjunto, essas decisões refletem o esforço institucional de equilibrar liberdade de expressão e proteção de direitos fundamentais no ambiente digital, especialmente quando se trata de grupos historicamente vulnerabilizados.

3. MAL-ESTAR DIGITAL E PROCESSOS DE EXCLUSÃO

3.1. Hipervulnerabilidade como construção estrutural

A noção de hipervulnerabilidade no espaço digital ultrapassa a ideia clássica de fragilidade individual. Do ponto de vista sociológico, trata-se de um processo social e relacional, no qual as condições históricas, econômicas e culturais produzem sujeitos expostos a riscos acentuados.

A literatura organiza as respostas à hipervulnerabilidade digital em quatro eixos: jurídico (ECA, LGPD e marcos europeus), social (redes de solidariedade), educacional (mediação parental e alfabetização digital) e institucional (cooperação entre governos, escolas e plataformas).

Apesar de avanços na literatura, persistem lacunas quanto à análise da hipervulnerabilidade de idosos e pessoas com deficiência, ainda pouco abordadas nas pesquisas (IZQUIERDO MONTERO et al., 2022). Os estudos concentram-se em crianças, adolescentes e mulheres, apontando múltiplos danos — exclusão digital, violência simbólica, cyberbullying e discurso de ódio — que se intensificam em contextos marcados por pobreza, discriminação e legados coloniais (ESPINOSA ZÁRATE et al., 2023; CORREIA, 2023; PONTE et al., 2023). Tais riscos revelam como o colonialismo de dados e a lógica algorítmica reforçam desigualdades pré-existent, ampliando a exposição de grupos historicamente vulneráveis (SILVEIRA, 2021).

A literatura aponta que pobreza, desigualdade e barreiras culturais ampliam a hipervulnerabilidade digital em comunidades de baixa renda na América Latina e no sul da Europa, especialmente entre meninas e crianças mais novas (ESPINOSA ZÁRATE et al., 2023; PONTE et al., 2023). Fragilidade dos marcos regulatórios frente ao discurso de ódio aparece como fator agravante em contextos de crise econômica e crescimento de partidos nacionalistas (IZQUIERDO MONTERO et al., 2022).

As plataformas digitais apresentam riscos distintos que intensificam a hipervulnerabilidade de grupos já fragilizados. Redes como Instagram, Twitter, YouTube e Facebook potencializam a superexposição, violações de privacidade, cyberbullying e discurso de ódio, especialmente contra mulheres, migrantes e minorias (CORREIA, 2023; IZQUIERDO MONTERO et al., 2022; QUARESMA et al., 2024). Pesquisas também indicam que a interseção entre gênero, etnicidade e classe aumenta as barreiras de inclusão digital e a incidência de violência simbólica, afetando de modo particular mulheres negras, jovens indígenas e meninas mais novas (ESPINOSA ZÁRATE et al., 2023; PONTE et al., 2023).

Apesar desses avanços, ainda são escassos os estudos sobre idosos e pessoas com deficiência, grupos igualmente expostos à hipervulnerabilidade digital. A literatura recomenda ampliar o foco das políticas públicas e das pesquisas para contemplar esses segmentos e fortalecer a avaliação da efetividade das estratégias de prevenção (IZQUIERDO MONTERO et al., 2022; ESPINOSA ZÁRATE et al., 2023; LIMA et al., 2025).

3.2 Impactos do mal-estar contemporâneo no ambiente digital

Pesquisas recentes ajudam a compreender como o mal-estar digital se articula ao excesso de visibilidade, à pressão algorítmica e à ausência de mediações simbólicas. Rodrigues (2020) demonstra que, durante a pandemia, os algoritmos intensificaram controle e vigilância, reforçando o mal-estar vinculado à observação constante de corpos e mentes. Na mesma direção, Oliveira (2023) evidencia, por meio de entrevistas e um atlas visual colaborativo, como regimes de visibilidade estruturam exclusões e invisibilidades.

Estudos empíricos internacionais reforçam esses efeitos. Galeazzi et al. (2024) mostram que variações algorítmicas reduzem a visibilidade de conteúdos no Twitter, enquanto Santana (2021) destaca o caráter não neutro dos algoritmos, impregnados por interesses econômicos e culturais que ampliam a hipervulnerabilidade digital. Campanella (2023) acrescenta que as plataformas reorganizam quem aparece e quem é invisibilizado, substituindo mediações tradicionais, como escola e família, por circuitos de performance e recompensa baseados em curtidas e tendências, que alimentam ansiedade e medo da exclusão.

No campo empírico brasileiro, Araújo e Silva (2023) e Pithan e Closs (2024) analisam como os trending topics e mecanismos de ranqueamento configuram uma governança invisível do comportamento digital. A opacidade das plataformas evidencia a fragilidade das mediações simbólicas diante do poder algorítmico. Silva (2025) complementa ao demonstrar como a formação de bolhas informacionais reforça vieses e sentimentos de isolamento, moldando percepções e comportamentos.

Pesquisas mais recentes associam diretamente os mecanismos de amplificação e ocultação de conteúdos ao sofrimento digital, manifestado em ansiedade, exclusão e silenciamento (SANTOS et al., 2025). Em plataformas como o TikTok, a invisibilização de criadores negros perpetua desigualdades históricas e insegurança econômica (OLIVEIRA, 2025). Entre adolescentes e influenciadores, a curadoria opaca das redes está associada à ansiedade, depressão e fragmentação identitária (GOMES et al., 2021; SANTOS et al., 2023; SANTOS et al., 2024; ABREU et al.,

2022). Estratégias de adaptação, como as chamadas gambiarras, revelam tentativas de contornar a lógica algorítmica (SANTOS; DALMOLIN, 2025), enquanto estudos sobre discriminação evidenciam barreiras estruturais à expressão (ROCHA et al., 2020).

Em perspectiva teórica, análises sobre estereótipos raciais e de gênero em bancos de imagens (CARRERA, 2020) e sobre governamentalidade algorítmica em patentes da Meta (ALVES; GOUVÊA, 2024) confirmam que as redes sociais intensificam o sofrimento subjetivo e a desigualdade digital nas realidades brasileiras e latino-americanas.

3.3 Dinâmicas de exclusão, violência simbólica e sofrimento psíquico

O ambiente digital, ao mesmo tempo em que amplia possibilidades de expressão, intensifica exclusões e sofrimentos psíquicos. Pesquisas no Brasil mostram que a curadoria algorítmica amplifica discursos de ódio e cria bolhas informacionais que silenciam mulheres, negros, adolescentes e influenciadores, gerando experiências de invisibilização e violência simbólica (SANTOS et al., 2025; OLIVEIRA, 2025; ROCHA et al., 2020). Esses processos afetam diretamente a saúde mental, associando-se a ansiedade, depressão e fragmentação identitária (GOMES et al., 2021; ABREU et al., 2022; SANTOS et al., 2023; SANTOS et al., 2024).

Sob a ótica psicanalítica, Freud (1930/2010) já apontava que o mal-estar na cultura decorre do conflito entre pulsões individuais e exigências sociais, tensão essa radicalizada no ambiente digital. Lacan (1969/2003), ao formular o discurso do capitalista, ajuda a compreender como os algoritmos funcionam como engrenagens de aceleração do gozo: oferecem objetos simbólicos como likes, seguidores, visualizações que prometem satisfação imediata e reiniciam continuamente o desejo.

Birman (2006, 2016) e Gaulejac (2007) descrevem como o excesso de gozo, a solidão digital e a internalização das normas de desempenho convertem-se em precariedade subjetiva e mal-estar cotidiano. Assim, a hipervulnerabilidade digital não se limita à exposição de dados, mas constitui uma engrenagem psíquica e social que transforma redes de interação em espaços de sofrimento simbólico e afetivo.

4. INCLUSÃO DIGITAL E CIDADANIA

4.1. Inclusão digital como direito humano

A educação é um direito fundamental garantido pela Constituição Federal de 1988 (arts. 5º e 205) e regulamentado pela Lei de Diretrizes e Bases da Educação Nacional (LDB n. 9.394/1996). A

educação digital constitui desdobramento desse direito, articulando-se ao direito de acesso à informação (art. 19 da Declaração Universal dos Direitos Humanos) e às metas da Agenda 2030, especialmente à ODS 4 (educação de qualidade) e à ODS 9 (inovação e infraestrutura). Nesse contexto, a Política Nacional de Educação Digital (PNED), instituída pela Lei n. 14.533/2023, torna obrigatório o componente curricular de educação digital no ensino fundamental e médio, em consonância com o Marco Civil da Internet (2014) e a Lei Geral de Proteção de Dados (LGPD, 2018).

O desenvolvimento da inclusão digital, contudo, deve ir além da infraestrutura tecnológica: trata-se de condição para o exercício da cidadania e da participação política. No campo escolar, isso implica promover mediações pedagógicas que estimulem o letramento digital crítico, a ética informacional e a compreensão de como plataformas e algoritmos estruturam a circulação do conhecimento (VAN DIJCK et al., 2018). Essa abordagem reafirma os princípios constitucionais do direito à educação e à informação como fundamentos da participação social no ambiente digital.

Dados recentes indicam que sete em cada dez estudantes do ensino médio já utilizam ferramentas de Inteligência Artificial Generativa em suas atividades escolares, muitas vezes sem mediação docente (Cetic.br, TIC Educação, 2024). Esse cenário evidencia que a inclusão digital não pode se restringir à dimensão técnica: deve articular-se às dimensões pedagógica, ética, política, cultural e filosófica, favorecendo o desenvolvimento do pensamento crítico no processo educativo.

4.2. Dados sobre alfabetização digital no Brasil (crianças, idosos, mulheres, PcD)

Partindo da concepção de alfabetização como prática social (SOARES, 2024), o letramento digital crítico deve preparar crianças e adolescentes para navegar na internet com segurança, ética e responsabilidade. Iniciativas como o TIC Kids Online Brasil e as ações do NIC.br oferecem subsídios importantes para políticas públicas. Em 2024, 65% dos jovens já utilizavam ferramentas de inteligência artificial generativa para estudar, criar conteúdo e lidar com emoções (Cetic.br, TIC Educação, 2024), o que evidencia a necessidade de mediação pedagógica e familiar.

O acesso à internet ocorre cada vez mais cedo: 24% das crianças acessaram pela primeira vez até os seis anos, e 88% dos jovens de 9 a 17 anos possuem perfis em plataformas como YouTube, WhatsApp, Instagram e TikTok (TIC Kids Online, 2025). Essa presença precoce em ambientes de coleta e monetização de dados (ZUBOFF, 2019) exige ações de formação digital crítica voltadas a professores, estudantes e famílias, para reduzir riscos e promover uso ético e consciente das tecnologias.

Quanto aos riscos, 17% dos usuários entre 11 e 17 anos relataram incômodo após contato com mensagens de teor sexual (TIC Kids Online, 2025), o que reforça a urgência de estratégias educativas que envolvam diálogo entre escola e família.

No panorama populacional, 88% dos brasileiros com 10 anos ou mais usaram a internet em 2023; entre idosos (60+), o índice foi de 66%. O celular é o principal meio de acesso (98,8%), seguido da TV (49,8%) e do microcomputador (34,2%) (TIC Domicílios, 2023). Ainda assim, 12 milhões de lares permanecem sem conexão, por motivos de custo, falta de habilidade ou desinteresse. Para pessoas com deficiência, a exclusão digital é agravada pela inacessibilidade: apenas 2,9% dos sites brasileiros atenderam plenamente aos critérios de acessibilidade em 2024 (IBGE, 2024).

Esse quadro confirma a hipervulnerabilidade digital em diferentes faixas etárias e grupos sociais. Embora 31% dos jovens afirmem ajudar seus pais em atividades on-line, apenas 44% dos responsáveis relatam dialogar com seus filhos sobre o uso da rede (TIC Kids Online, 2025). Esses dados reforçam que a inclusão digital ultrapassa o acesso técnico: trata-se de um processo pedagógico, cultural e social que requer formação crítica e políticas inclusivas contínuas.

4.3. Experiências e programas de educação digital para prevenção e fortalecimento da cidadania.

A educação digital, articulada ao letramento midiático-informacional, constitui uma prática educativa essencial para prevenir cyberbullying, desinformação, golpes, assédio e violências digitais, promovendo a ética e a cidadania nos ambientes virtuais. Nesse contexto, destacam-se programas nacionais e estratégias de inclusão como o Programa Computadores para Inclusão, os Centros de Recondicionamento de Computadores (CRCs) e as iniciativas do NIC.br e do Cetic.br.

O Programa Computadores para Inclusão, coordenado pelo Governo Federal, fomenta a inclusão digital por meio dos CRCs, espaços destinados à formação, oficinas e conscientização sobre o uso e o descarte sustentável de equipamentos eletrônicos. Em 2024, registrou mais de 14 mil doações de equipamentos e 10 mil participantes em cursos e oficinas, ampliando o acesso à cidadania digital e à cultura de segurança.

O NIC.br/Cetic.br disponibiliza materiais educativos como a Cartilha de Segurança para a Internet e guias de boas práticas voltados a professores, estudantes e comunidades escolares. Também produz indicadores nacionais (TIC Kids Online, TIC Domicílios e TIC Educação) que orientam políticas públicas e estratégias pedagógicas de alfabetização digital. O Programa Educação

Conectada, do MEC, complementa essas ações ao apoiar infraestrutura e uso pedagógico de tecnologias digitais nas escolas públicas.

Em âmbito internacional, a UNESCO promove o letramento midiático-informacional (MIL) por meio de currículos e diretrizes para políticas públicas, como o Currículo MIL para Professores e a Semana Global MIL, além de coleções de recursos abertos sobre desinformação, privacidade e cidadania digital (UNESCO, 2013; 2021; 2024). Esses materiais orientam redes de ensino a integrar competências críticas e participativas no currículo da educação básica e superior.

Assim, a educação digital se configura como um instrumento estratégico de prevenção e de redução da hipervulnerabilidade nos ambientes digitais, fortalecendo a cidadania e a responsabilidade coletiva no uso ético das tecnologias (UNESCO, 2021).

5. CONCLUSÃO

A hipervulnerabilidade digital, compreendida como fenômeno estrutural e relacional, demanda respostas integradas entre o campo jurídico, o educacional e o social. As análises apresentadas indicam que, embora o Brasil possua um arcabouço normativo robusto com destaque para a Constituição, a LGPD, o Marco Civil da Internet e o novo ECA Digital, ainda há um hiato entre a existência das normas e sua efetividade. A proteção de dados, a transparência algorítmica e a responsabilização das plataformas permanecem desafios centrais.

Sob o olhar da sociologia clínica e da psicanálise, observa-se que os algoritmos potencializam o mal-estar contemporâneo ao converterem visibilidade em valor e desejo de reconhecimento, criando novas formas de exclusão simbólica. Assim, a hipervulnerabilidade digital não se limita à dimensão técnica da segurança, mas abrange processos subjetivos e culturais que afetam o laço social e a constituição do sujeito.

No campo educacional, a alfabetização digital crítica emerge como instrumento essencial de cidadania. A formação para o uso ético, seguro e responsável das tecnologias deve ser vista como política pública de prevenção, capaz de reduzir desigualdades e fortalecer a autonomia dos usuários.

Conclui-se que enfrentar a hipervulnerabilidade digital requer uma governança ética e interdisciplinar, pautada em valores de justiça social, inclusão e cuidado. É preciso articular legislação, educação e suporte psicológico-social, criando um ecossistema digital mais humano e sustentável, no qual a inovação tecnológica caminhe lado a lado com a dignidade e a proteção dos sujeitos.

REFERÊNCIAS

- ABREU, Liliane Alcântara de; MELO, Natalia Sayuri; SOARES, Pamela Cristina de Souza; NUNES, Letícia Monteiro; SILVA, Gabriella Braga Dias da; MENDES, Matheus Passos. As influencers digitais e a autoimagem como produto de comportamento de consumo. *Revista Científica Multidisciplinar Núcleo do Conhecimento*, v. 7, n. 11, p. 3071–3095, 2022. Disponível em: <https://www.nucleodoconhecimento.com.br/psicologia/comportamento-de-consumo>
- ALMAPRETA. *Redes sociais devem remover conteúdos de racismo, pedofilia e discurso de ódio, decide STF*. Disponível em: <https://almapreta.com.br/sessao/cotidiano/redes-sociais-devem-remover-conteudos-de-racismo-pedofilia-e-discurso-de-odio-decide-stf/>.
- ALVES, Marco Antônio Sousa; GOUVEA, Ane Laura Rios. Patenteando subjetividades. *Revista do CAAP*, v. 14, n. 2, p. 217–240, 2024. Disponível em: <https://revistas.usp.br/matrizes/article/view/167187>
- ARAÚJO, Rafael de Paula Aguiar; SILVA, Igor Fediczko. A capacidade dos trending topics em pautar o debate: agenda setting do algoritmo. *Cadernos Metrópole*, São Paulo, v. 25, n. 58, p. 1123–1142, 2023. Disponível em: <https://www.scielo.br/j/cm/a/pk6nHfWmnWWvP3wv86Jrz7C/?format=html&lang=pt>
- BIRMAN, Joel. *Mal-estar na atualidade: a psicanálise e as novas formas de subjetivação*. Rio de Janeiro: Civilização Brasileira, 2006.
- BIRMAN, Joel. *O sujeito na contemporaneidade: espaço, dor e desalento na atualidade*. Rio de Janeiro: Civilização Brasileira, 2016.
- BRASIL. *Constituição (1988). Constituição da República Federativa do Brasil de 1988*. Brasília, DF: Senado Federal, 1988.
- BRASIL. Governo Federal. *Misoginia: mulheres são vítimas de ataques e violações de direitos na internet*. Brasília: Ministério dos Direitos Humanos e da Cidadania, 2024. Disponível em: <https://www.gov.br/mdh/pt-br/assuntos/noticias/2024/julho/misoginia-mulheres-sao-vitimas-de-ataques-e-violacoes-de-direitos-na-internet>
- BRASIL. *Lei nº 12.965, de 23 de abril de 2014*. Marco Civil da Internet. Diário Oficial da União, Brasília, 2014.

BRASIL. *Lei nº 13.709, de 14 de agosto de 2018*. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, Brasília, 2018.

BRASIL. *Lei nº 14.533, de 11 de janeiro de 2023*. Institui a Política Nacional de Educação Digital (PNED). Diário Oficial da União, Brasília, 2023.

BRASIL. *Lei nº 9.394, de 20 de dezembro de 1996*. Estabelece as diretrizes e bases da educação nacional. Diário Oficial da União, Brasília, 1996.

BRASIL. Secretaria de Segurança da Informação e Cibernética (GSI/PR). *Manual de Segurança Digital – Fascículo: Violência cibernética contra as mulheres*. Brasília, 2024. Disponível em: https://www.gov.br/gsi/pt-br/seguranca-da-informacao-e-cibernetica/fasciculos/fasciculo_violencia_cibernetica_contra_as_mulheres.pdf. Acesso em: 29 out. 2025.

BRASIL. Secretaria de Segurança da Informação e Cibernética (GSI/PR). *Manual de Segurança Digital*. Fascículo: Violência cibernética contra as mulheres. Brasília, 2024. Disponível em: https://www.gov.br/gsi/pt-br/seguranca-da-informacao-e-cibernetica/fasciculos/fasciculo_violencia_cibernetica_contra_as_mulheres.pdf

BRASIL. Superior Tribunal de Justiça (STJ). Relator: Ministro Antonio Carlos Ferreira. *Provedor deve remover conteúdo ofensivo a menor na internet, mesmo sem ordem judicial*. Brasília, 16 dez. 2021. Disponível em: <https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/16122021-Provedordeve-remover-conteudo-ofensivo-a-menor-na-internet--mesmo-sem-ordem-judicial.aspx>. Acesso em: 29 out. 2025.

BRASIL. Superior Tribunal de Justiça (STJ). Relator: Ministro Antonio Carlos Ferreira. *Provedor deve remover conteúdo ofensivo a menor na internet, mesmo sem ordem judicial*. Brasília, 16 dez. 2021. Disponível em: <https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/16122021-Provedordeve-remover-conteudo-ofensivo-a-menor-na-internet--mesmo-sem-ordem-judicial.aspx>

BRASIL. Tribunal Superior Eleitoral (TSE). *Justiça Eleitoral responsabilizará autores de notícias falsas com ou sem uso de IA nas eleições, diz presidente do TSE*. Brasília, 2 abr. 2024. Atualizado em: 7 mar. 2025. Disponível em: <https://www.tse.jus.br/comunicacao/noticias/2024/Abril/justica-eleitoral-responsabilizara-autores-de-noticias-falsas-com-ou-sem-uso-de-ia-nas-eleicoes-diz-presidente-do-tse-1>

CAMPANELLA, Bruno. Regimes de visibilidade nas plataformas digitais: uma leitura sociológica. *Revista Famecos*, Porto Alegre, v. 30, n. 1, p. 1–20, 2023. Disponível em:

<https://www.scielo.br/j/gal/a/zJKgKbz8pYJLWKbHrkcDGKJ/?lang=pt&format=pdf>

CARRERA, Fernanda. A raça e o gênero da estética e dos afetos: algoritmização do racismo e do sexismo em bancos contemporâneos de imagens digitais. *MATRIZES*, v. 14, n. 2, p. 217–240, 2020.

Disponível em: <https://revistas.usp.br/matrizes/article/view/167187>

CORREIA, Amanda Baraúna. Responsabilidade civil dos pais nos casos de hiperexposição infantil em plataformas digitais no Brasil. *Revista Conversas Civilísticas*, v. 3, n. 0, p. 1–25, 2023.

Disponível em: <https://periodicos.ufba.br/index.php/conversascivilisticas/article/view/54871>

ESPINOSA ZÁRATE, Zaida; CAMILLI TRUJILLO, Celia; PLAZA-DE-LA-HOZ, Jesús.

Digitalization in vulnerable populations: A systematic review in Latin America. *Social Indicators Research*, v. 168, n. 2, p. 567–590, 2023. Disponível em:

<https://link.springer.com/article/10.1007/s11205-023-03239-x>

FREUD, Sigmund.(1930). *O mal-estar na cultura*. São Paulo: Companhia das Letras, 2010.

GALEAZZI, Alessandro; PAUDEL, Pujan; CONTI, Mauro; , CRISTOFARO, Emiliano De, STRINGHINI, Gianluca. *Revealing the Secret Power: How Algorithms Can Influence Content Visibility on Social Media*. arXiv preprint arXiv:2410.17390, 2024. Disponível em:

<https://arxiv.org/abs/2410.17390>.

GAULEJAC, Vincent de. *A sociedade do mal-estar: coaching, gestão e capitalismo*. Petrópolis: Vozes, 2007.

GOMES, Gêisa Cláudia; SANTOS, K.; SOUZA, Yara Evelyng Rabelo; NASCIMENTO, Gilmar dos Santos. Impactos da pandemia de COVID-19 para a visibilidade da cultura do cancelamento nas redes sociais. *Revista Ibero-Americana de Humanidades, Ciências e Educação*, v. 7, n. 11, p.

3071–3095, 2021. Disponível em: <https://periodicorease.pro.br/rease/article/view/3071>

INSTITUTO BRASILEIRO DE DIREITO DE FAMÍLIA (IBDFAM). *Registros de cyberbullying aumentam um ano após inclusão no Código Penal*. 7 abr. 2025. Disponível em:

<https://ibdfam.org.br/noticias/12780/Registros+de+cyberbullying+aumentam+um+ano+ap%C3%B3s+inclus%C3%A3o+no+C%C3%B3digo+Penal>.

IZQUIERDO MONTERO, Alberto; LAFORGUE-BULLIDO, Noemi; ABRIL-HERVÁS, David. Hate speech: A systematic review of scientific production and educational considerations. *Revista*

Fuentes, v. 24, n. 2, p. 153–176, 2022. Disponível em:

https://institucional.us.es/revistas/fuente/24_2/Art_9.pdf

LABIO-BERNAL, Antonio; ROMERO-DOMÍNGUEZ, Lorena R.; GARCÍA-ORTA, María José.

Protection of minors in the European digital audiovisual context: A necessary dialogue between parents, academy, regulators and industry. *Comunicación y Sociedad*, v. 37, p. 1–20,

2020. Disponível em: <https://revistacomsoc.pt/article/view/2162>

LACAN, Jacques. *O Seminário, livro 17: O avesso da psicanálise* (1969–1970). Rio de Janeiro: Zahar, 2003.

LIMA, Geisiane Sousa; FABRICIO, Lenira Feras da Silva; NASCIMENTO, Fernando Jorge Souza do; SOUZA, Ingryd Stéphanie Monteiro de. Fórum digital: o acesso à justiça como direito fundamental. *Revista Ft*, v. 10, n. 2, p. 42–59, 2025. Disponível em:

<https://revistaft.com.br/forum-digital-o-acesso-a-justica-como-direito-fundamental/>

NEXO JORNAL LTDA; SCHMIDT, Sarah. *Ataques cibernéticos a universidades e instituições científicas crescem no país*. *Revista Pesquisa Fapesp*, São Paulo, jun. 2025. Disponível em:

<https://www.nexojournal.com.br/externo/2025/06/16/ataque-hacker-universidade-e-pesquisas-cientificas-aumenta-no-brasil>.

OCDE. Organização para a cooperação e desenvolvimento econômico. *Artificial Intelligence in Society*. Paris: OECD Publishing, 2020. DOI: <https://doi.org/10.1787/eedfee77-en>

OLIVEIRA, Marcos Leandro Silva. A invisibilidade digital dos influenciadores negros no Brasil. *Temáticas*, v. 33, n. 65, p. 1–20, 2025. Disponível em:

<https://econtents.sbu.unicamp.br/inpec/index.php/tematicas/article/view/19945>

OLIVEIRA, Raquel Assunção. Regimes of visibility and algorithmic surveillance on digital platforms: operationalizing the thought through images in a collaborative perspective. *Journal of Latin American Communication Research*, v.11, n.2, 2023. Disponível em:

<https://journal.pubalaic.org/index.php/jlacr/article/view/160>.

PITHAN, Liana Haygert; CLOSS, Lisiane Quadrado. Gestão invisível do trabalho orientado à visibilidade: governança por plataformas de mídia social. *ERA. Revista de Administração de Empresas*, São Paulo, v. 64, n. 6, p. 1-25, 2024. Disponível em:

<https://www.scielo.br/j/rae/a/Sw6nsYT5mdMdxqbtjSfZ84n/?lang=pt>

PONTE, Cristina; MASCHERONI, Giovanna; BATISTA, Susana; GARMENDIA, Maialen;

MARTÍNEZ, Gemma; CINO, Davide. Children’s digital mediation: The family climate in Spain,

Italy and Portugal. *Observatorio (OBS*)*, v. 17, n. 2, p. 214–235, 2023. Disponível em:

<https://obs.obercom.pt/index.php/obs/article/view/2214>

QUARESMA, Vitória Maria Cezário; SUASSUNA, Maria Aparecida Ferreira; ABREU, Hilana Maria Braga Fernandes; TEMÓTEO, Lúcia Maria. Technology and sexual abuse – The role of technology in facilitating child and adolescent sexual abuse: A systematic review. *Revista Interdisciplinar e do Meio Ambiente (RIMA)*, v. 6, n. 1, p. 1–25, 2024. Disponível em:

<https://caroa.org.br/revista/index.php/rima/article/view/236>

ROCHA, C. J.; PORTO, L. V.; ABAURRE, Helena Emerick. Discriminação algorítmica no trabalho digital. *Revista Sociedade Científica*, v. 1, n. 1, p. 1–15, 2020. Disponível em:

<https://periodicos.puc-campinas.edu.br/direitoshumanos/article/view/5201>

RODRIGUES, Marcelo Gonçalves. Algoritmos de Mal-Estar: Ciberpandemia e Privacidade Hackeada. *Revista de Filosofia Moderna e Contemporânea*, Brasília, v.8, n.3, dez. 2020, p. 105-136. Disponível em: <https://periodicos.unb.br/index.php/fmc/article/view/34499/28804>

SANTANA, Ramon Davi. Rastros na rede: as práticas de modulação algorítmica. *Dissertação* (Mestrado em Comunicação e Cultura Contemporâneas) – Universidade Federal da Bahia, Salvador, 2021. Disponível em:

<https://repositorio.ufba.br/bitstream/ri/37924/5/Disserta%C3%A7%C3%A3o.%20Ramon%20Davi%20Santana.pdf>.

SANTOS, Anísio Miranda dos; COELHO, Matheus Garcia; RESGALA JÚNIOR, Renato Marcelo. Modulação social e os desdobramentos psicopatológicos que atravessam os nativos digitais inseridos no ciberespaço da internet, numa perspectiva fenomenológica existencial. *Revista Sociedade Científica*, v. 1, n. 1, p. 1–20, 2023. Disponível em:

<https://revista.scientificsociety.net/wp-content/uploads/2023/10/Art.207-2023.pdf>

SANTOS, Jéssica Caroline Pessoa dos; SOUZA, Alice Andrade de; CORRÊA, Bruna Guedes; MELO, Gabriel Cavalcanti; SODRÉ, Giovanna Erculano. Subjetividade digital em adolescentes na pandemia: um olhar da Psicologia Analítica. *Psicologia Argumento*, v. 42, n. 117, p. 1–20, 2024.

Disponível em: <https://periodicos.pucpr.br/psicologiaargumento/article/view/31192>

SANTOS, Kassieli Joaquina Gonçalves de Mello dos; DALMOLIN, A. Impacto dos algoritmos na performance dos influenciadores digitais: gambiarras e visibilidade. *Ação Midiática: Estudos em Comunicação, Sociedade e Cultura*, v. 29, n. 1, p. 1–20, 2025. Disponível em:

<https://revistas.ufpr.br/acaomidiatica/article/view/96934>

SCHMIDT, Sarah. Ataques cibernéticos a universidades e instituições científicas crescem no país.

São Paulo: Nexo Jornal Ltda; *Revista Pesquisa Fapesp*, jun. 2025. Disponível em:

<https://www.nexojournal.com.br/externo/2025/06/16/ataque-hacker-universidade-e-pesquisas-cientificas-aumenta-no-brasil>

SILVA, Laercio; ROCHA, Francisco; BALUZ, Rodrigo Augusto. A formação das bolhas informacionais na comunicação digital: Uma revisão bibliográfica sobre as métricas algorítmicas dentro das redes sociais Facebook, Twitter e TikTok. *Revista Eletrônica de Iniciação Científica em Computação*, v.23, n.1, p.16–23, 2025. Disponível em:

https://journals-sol.sbc.org.br/index.php/reic/article/view/5402?utm_source=chatgpt.com

SILVEIRA, Sérgio Amadeu da. A hipótese do colonialismo de dados e o neoliberalismo. IN:

SILVEIRA, Sérgio Amadeu da; SOUZA, Joyce; CASSIANO, João. (orgs.). *Colonialismo de dados: como opera a trincheira algorítmica na guerra neoliberal*. São Paulo: Autonomia Literária, 2021. p. 33-51.

SOARES, Magda. B. Letramento e alfabetização: as muitas facetas. *Revista Brasileira de Educação*, Rio de Janeiro, n. 25, p. 5-17, 2004. DOI:

<http://dx.doi.org/10.1590/S1413-24782004000100002>

VAN DIJCK, José; POELL, Thomas; DE WAAL, Martijn. *The platform society: Public values in a connective world*. Oxford University Press, 2018.

ZUBOFF, S. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: Public Affairs, 2019.