A SOCIEDADE DA CAIXA PRETA E A VIOLÊNCIA CIBERNÉTICA: O SEGREDO DE NEGÓCIO ALGORÍTMICO COMO ÓBICE À EFICÁCIA DO MARCO CIVIL DA INTERNET DIANTE DE MÍDIAS SINTÉTICAS

Brunna Victória Conceição de Jesus[1], Rhara Vitória de Araújo Barros Santos[2], André Luiz de Andrade Ferreira[1,2], Gabriel Vinicius Andrade Santos[1,3], Ana Beatriz Santos Mecenas[1,4]

[1]Centro Universitário Estácio de Sá de Sergipe, Aracaju, Brasil
(brunnavictoria550@gmail.com)
[2]Universidade Tiradentes (UNIT), Aracaju, Brasil

Resumo: O artigo analisa a responsabilidade das plataformas ante mídias sintéticas (*deepfakes*). Sob o Marco Civil da Internet, aponta-se a ineficácia do art. 19 frente à velocidade da IA, gerando uma inversão axiológica: protege-se a propriedade intelectual de forma célere, mas submete-se a dignidade humana à morosidade judicial. Critica-se o uso do segredo de negócio como escudo para a inércia, propondo sua flexibilização para conter preventivamente a violência cibernética.

Palavras-chave: Propriedade Industrial; Segredo de Negócio; Marco Civil da Internet; Mídias Sintéticas; Violência Cibernética.

INTRODUÇÃO

A virada tecnológica operada pela consolidação e massificação da Inteligência Artificial (IA) generativa transformou profundamente a infraestrutura de produção, circulação e consumo de conteúdos no ambiente digital. O surgimento de sistemas complexos de síntese audiovisual dotados de interfaces gráficas intuitivas e de baixo custo operacional promoveu a denominada "comoditização" da tecnologia (Kesavarajah *et al*., 2025).

Esse fenômeno reduziu drasticamente as barreiras de entrada técnica e financeira, permitindo que usuários leigos manipulem algoritmos avançados para a criação de representações digitais hiper-realistas. Contudo, em que pese os benefícios socioeconômicos advindos da inovação computacional, essa massificação descortinou novos e alarmantes contornos para a violência cibernética no ecossistema virtual.

Dentre as manifestações mais lesivas desse avanço, destaca-se a proliferação das mídias sintéticas manipuladas, popularmente conhecidas como *deepfakes*. Valendo-se de técnicas de aprendizado profundo (*deep learning*), essas ferramentas detêm a capacidade de recriar digitalmente elementos intrínsecos à identidade humana, tais como a fisionomia corporal, os movimentos faciais e a modulação da voz (Ajder *et al*., 2019).

A atual sofisticação algorítmica oblitera as fronteiras entre o fato autêntico e a fabricação digital, expondo o cidadão comum a um estado de vulnerabilidade constante no que tange aos seus direitos da personalidade, gerando um ambiente propício para a desinformação e a difamação em larga escala (Ajder *et al*., 2019).

A velocidade incontrolável com que essas mídias sintéticas trafegam nas redes sociais evidencia a crônica insuficiência do microssistema de responsabilidade civil desenhado pelo Marco Civil da Internet (Brasil, 2014).

A regra geral insculpida no artigo 19 da referida legislação condiciona a responsabilização civil das plataformas digitais à prévia desobediência de uma ordem judicial específica para a remoção do conteúdo ilícito. Esse modelo estritamente reativo impõe à vítima um severo ônus procedimental e temporal, totalmente incompatível com o dinamismo do ciberespaço (Pinheiro, 2021).

É precisamente diante desse gargalo operativo e temporal que a adoção de medidas preventivas pelas próprias plataformas se torna imperiosa. Contudo, quando instadas pelo Poder Público ou pelos usuários a implementar filtros algorítmicos para conter a

difusão prévia de conteúdos manifestamente degradantes, as transnacionais de tecnologia blindam-se sob a égide da Lei de Propriedade Industrial (Brasil, 1996), amparando-se no "segredo de negócio" de suas arquiteturas algorítmicas.

Consolida-se, sob essa retórica corporativa, a denominada "sociedade da caixa preta" (Pasquale, 2015), na qual a opacidade estrutural dos sistemas computacionais impede a auditoria externa e neutraliza a eficácia horizontal dos direitos fundamentais, convertendo o ativo mercadológico empresarial em um escudo intransponível contra a responsabilidade social (Zuboff, 2019).

Essa assimetria protetiva consolida uma intolerável inversão axiológica no ordenamento jurídico brasileiro (Schreiber, s.d.). Enquanto o ecossistema digital disponibiliza ferramentas automatizadas e canais extrajudiciais céleres para estancar, em tempo real, violações a direitos autorais e marcas — priorizando a salvaguarda da propriedade imaterial mercadológica —, as ofensas aos atributos mais íntimos e existenciais da personalidade humana permanecem reféns da morosidade inerente aos trâmites do Poder Judiciário.

Diante do exposto, o objetivo geral deste artigo é investigar a tensão jurídica entre a proteção conferida aos segredos de negócio algorítmicos e a necessidade de interrupção imediata da violência cibernética mediada por mídias sintéticas.

Busca-se delimitar os impactos das adulterações tecnológicas sobre a identidade digital, examinar a insuficiência normativa do artigo 19 do Marco Civil da Internet e propor a flexibilização do sigilo industrial como pressuposto para a consagração de um dever de cuidado proativo por parte das plataformas digitais (Leonardi, 2005).

MATERIAL E MÉTODOS

Para compreender a complexidade sociotécnica e jurídica que envolve a proliferação de mídias sintéticas e a opacidade algorítmica, o presente estudo adota uma abordagem metodológica qualitativa, de natureza teórica, com objetivos exploratórios e descritivos.

O método de abordagem escolhido é o hipotético-dedutivo, partindo da premissa geral da primazia dos direitos fundamentais para analisar a hipótese de insuficiência protetiva do atual regime de responsabilidade civil da internet diante das novas tecnologias de manipulação audiovisual.

A abordagem qualitativa adotada pressupõe a análise crítica e interpretativa dos dados coletados, estabelecendo conexões interdisciplinares entre o Direito Civil, o Direito Digital e o Direito da Propriedade Industrial.

No que concerne aos procedimentos operacionais, a pesquisa estrutura-se a partir do levantamento bibliográfico e documental, executado em três etapas consecutivas e integradas:

A primeira etapa compreendeu a pesquisa bibliográfica, realizada por meio do mapeamento de livros de doutrina jurídica clássica e contemporânea, artigos científicos indexados em bases de dados acadêmicas (como Google Acadêmico e SciELO) e relatórios técnicos institucionais de relevância internacional.

Os critérios de busca e seleção de literatura delimitaram-se pelas palavras-chave "mídias sintéticas", "responsabilidade civil dos provedores", "segredo de negócio" e "direitos da personalidade". Priorizou-se a literatura crítica publicada entre os anos de 2013 e 2026, viabilizando o confronto teórico entre a teoria dos direitos existenciais e as dinâmicas econômicas da sociedade informacional e do capitalismo de vigilância.

A segunda etapa consistiu no levantamento e análise documental da legislação brasileira vigente. O escopo normativo concentrou-se no exame analítico da Lei nº 12.965/2014 (Marco Civil da Internet), especificamente no artigo 19, avaliando sua escolha político-legislativa e teleológica.

Esse arcabouço foi articulado de forma comparativa com o microssistema protetivo da Lei nº 9.279/1996 (Lei de Propriedade Industrial), com foco nas garantias conferidas ao segredo de negócio e à repressão da concorrência desleal, além do diálogo subsidiário com o Código Penal (Brasil, 1940).

A terceira e última etapa perfez o levantamento jurisprudencial focado nas decisões das cortes superiores brasileiras. Realizou-se uma busca sistemática nos repositórios digitais do Supremo Tribunal Federal (STF) e do Superior Tribunal de Justiça (STJ).

Os critérios de inclusão jurisprudencial fixaram-se em acórdãos paradigmáticos e *leading cases* julgados até o primeiro semestre de 2026, selecionando-se o Tema 533 da Repercussão Geral (STF) (Brasil, 2025) e Recursos Especiais (STJ) (Brasil, 2025) que debateram as fronteiras técnicas da moderação de conteúdo, a responsabilidade de intermediários e a relatividade do sigilo tecnológico empresarial.

Por fim, os dados e documentos obtidos foram submetidos ao método de análise de conteúdo e à hermenêutica constitucional. O procedimento interpretativo foi orientado pelo princípio da dignidade da pessoa humana e pela técnica de ponderação de interesses, permitindo diagnosticar a presença de assimetrias axiológicas no ordenamento e fundamentar a proposta de flexibilização do sigilo industrial algorítmico frente a lesões à identidade digital.

RESULTADOS E DISCUSSÃO

A aplicação prática dos institutos de responsabilização civil e de proteção à propriedade imaterial evidencia uma severa defasagem procedimental quando confrontada com o ritmo de difusão da Inteligência Artificial generativa (Pinheiro, 2021).

A discussão dos resultados estrutura-se a partir da identificação da ofensa sistêmica contra a identidade digital do cidadão, passando pela ineficácia da lei civil vigente, até culminar no conflito direto com os interesses mercadológicos e os segredos industriais das corporações tecnológicas.

Mídias Sintéticas e a Nova Era da Violência Cibernética: A Desconstrução da Identidade Digital

A proliferação massiva de mídias sintéticas geradas por sistemas de inteligência artificial generativa inaugurou uma era qualitativamente distinta e substancialmente mais nociva de violência cibernética. Se outrora os ilícitos praticados no ambiente virtual limitavam-se a manifestações textuais difamatórias ou à divulgação não autorizada de registros reais preexistentes, a engenharia reversa e o aprendizado profundo subverteram essa dinâmica ao conferir ao ofensor o poder de forjar fatos inteiramente inexistentes com traços inquestionáveis de realidade (Ajder et al., 2019).

Esse avanço opera o que a literatura classifica como a "armamentização" do algoritmo, transformando ferramentas computacionais em vetores de aniquilação reputacional e desestruturação psíquica do indivíduo (Kesavarajah *et al*., 2025). Essa facilidade técnica de manipulação audiovisual ampliou o escopo dos crimes cibernéticos, tornando o cidadão comum vulnerável a fraudes de identidade, extorsões e campanhas difamatórias hiper-realistas (Ajder *et al*., 2019).

Sob a óptica civil-constitucional, os danos irradiados por essas manipulações tecnológicas atingem o cerne dos direitos da personalidade. Conforme leciona a doutrina de Diniz (2022), o direito à imagem deve ser compreendido a partir de uma perspectiva dicotômica e complementar: a imagem-retrato, que abrange a projeção física, a fisionomia e os caracteres anatômicos estritos do indivíduo; e a imagem-atributo, representativa do conjunto de qualificações, virtudes, reputação e estima social cultivados pelo sujeito perante a coletividade. No contexto das mídias sintéticas baseadas em *deepfakes*, essa divisão teórica sofre um impacto cumulativo profundo.

O agente difusor usurpa a imagem-retrato da vítima, acoplando seu rosto e suas expressões faciais a cenários forjados de nudez, pornografia ou práticas ilícitas. Por via de consequência direta, essa adulteração material destrói de forma instantânea a imagem-atributo do indivíduo, gerando um estigma perante o meio social que oblitera qualquer capacidade de defesa imediata, dada a verossimilhança técnica da falsificação (Rodrigues, 2023).

Ademais, na perspectiva do Direito da Propriedade Intelectual e da governança informacional, esse processo de criação sintética escancara um conflito estrutural que retroalimenta a violência digital. Os modelos de linguagem e as redes neurais generativas não operam em um vácuo de dados; ao contrário, sua eficácia depende da extração massiva e automatizada de dados na internet, técnica conhecida como *data scraping* (Kesavarajah et al., 2025).

Nesse cenário, fotografias ordinárias, dados biométricos e registros de imagem publicados por usuários comuns em redes sociais são capturados indiscriminadamente pelas grandes corporações para servir de matéria-prima gratuita no treinamento de seus algoritmos comerciais (Zuboff, 2019). O corpo e a fisionomia do cidadão são convertidos em insumos mercadológicos sem qualquer consentimento, violando as balizas da autodeterminação informativa.

Configura-se, portanto, um ciclo de exploração no qual a imagem do indivíduo é expropriada para aperfeiçoar a própria tecnologia que, posteriormente,

será utilizada como instrumento de sua degradação moral e violação de sua privacidade recôndita (Nações Unidas, 2026).

A Crise de Eficácia do Marco Civil da Internet e a Inversão Axiológica

A superação das lesões digitais e o consequente estancamento dos danos à personalidade deparam-se com o anacronismo e o engessamento procedimental do modelo de responsabilidade civil estabelecido pela Lei nº 12.965/2014. Com o intuito original de salvaguardar a liberdade de expressão e impedir a censura prévia privada, o artigo 19 do referido diploma legal instituiu o regime de responsabilidade civil subjetiva condicionada. Sob essa sistemática, as plataformas digitais apenas respondem civilmente pelos danos decorrentes de conteúdos gerados por terceiros se, após a prolação de uma ordem judicial específica, permanecerem inertes e não adotarem as providências de remoção ou indisponibilização do material ilícito (Brasil, 2014).

Contudo, a transposição automática desse modelo reativo para a era da Inteligência Artificial generativa revela uma crônica insuficiência prática. Conforme adverte Pinheiro (2021), a variável temporal assume relevância crítica e existencial na sociedade da informação.

Subordinar a exclusão de mídias sintéticas altamente lesivas à morosidade inerente à obtenção de provimentos jurisdicionais impõe à vítima um ônus financeiro e temporal desproporcional, provocando o esvaziamento do próprio direito subjetivo que se busca tutelar (Pinheiro, 2021).

Na dinâmica das redes sociais, a dilação processual atua de forma diretamente proporcional à propagação da ofensa: enquanto o processo tramita nas instâncias do Poder Judiciário, os algoritmos de recomendação impulsionam o material de forma exponencial e global, transformando o ato isolado de postagem em um rastro perene e em um dano de natureza perpétua.

Essa sistemática processual culmina no fenômeno que Schreiber (2013) define de forma cirúrgica como uma "intolerável inversão axiológica" do ordenamento jurídico. O sistema legal brasileiro disponibiliza mecanismos tecnológicos automatizados e canais extrajudiciais ultravelozes para coibir infrações que atinjam direitos autorais e marcas de grandes conglomerados econômicos, dispensando qualquer crivo judicial prévio para a efetivação do bloqueio.

Todavia, quando o bem jurídico violado desloca-se da esfera patrimonial para a dimensão existencial da dignidade humana, da honra e da intimidade de um cidadão, o ordenamento retrocede e exige a via-crúcis burocrática do processo judicial como condição para a responsabilização da plataforma. Confere-se, abstratamente, uma tutela jurídica muito mais proativa e eficiente à propriedade imaterial mercadológica do que à integridade psíquica e moral da pessoa humana.

O Segredo de Negócio Algorítmico como Escudo para a Inércia Corporativa

O descompasso identificado entre o "tempo do processo judicial" e a "velocidade do algoritmo" agrava-se exponencialmente pela recusa sistemática das plataformas digitais em implementar filtros preventivos e mecanismos automatizados de bloqueio na origem.

Ao serem instadas por órgãos reguladores ou demandadas em juízo a adotar uma postura proativa, as grandes corporações tecnológicas invocam as garantias da Lei nº 9.279/1996 (Lei de Propriedade Industrial). Nos termos do referido diploma, o segredo de negócio visa tutelar conhecimentos, informações e dados técnicos ou comerciais confidenciais que conferem vantagem competitiva ao seu detentor, cuja divulgação ou exploração não autorizada configura ilícito de concorrência desleal (Brasil, 1996). Amparando-se nessa premissa, as plataformas argumentam que a arquitetura interna de seus sistemas de recomendação, seus códigos-fonte e seus moderadores neurais automáticos enquadram-se rigorosamente nesse escopo de proteção, formando um ativo intangível blindado contra interferências ou auditorias externas.

Sob essa justificativa concorrencial, consolida-se uma opacidade estrutural que serve de esteio para a manutenção do "capitalismo de vigilância", modelo econômico no qual a monetização do engajamento gerado por conteúdos sensacionalistas ou falsificados sobrepõe-se aos imperativos éticos e de segurança informacional (Zuboff, 2019).

Ocorre que o instituto do segredo de negócio e a proteção à propriedade industrial não possuem caráter absoluto no ordenamento jurídico pátrio, devendo submeter-se à sua função social e à supremacia dos direitos fundamentais. Conforme adverte Pasquale (2015), a falta de transparência em sistemas comerciais de grande escala impede o controle democrático e a responsabilização por danos coletivos, criando a opacidade característica da "sociedade da caixa preta".

Adicionalmente, leciona Leonardi (2005) que o dever de cuidado e a segurança jurídica impostos às

empresas prestadoras de serviços no ciberespaço não podem ser interpretados de forma estática, encontrando-se intrinsecamente vinculados ao "estado da técnica" disponível no momento histórico da atividade.

Partindo dessa premissa teórica, se as plataformas contemporâneas detêm capacidade técnica para mapear perfis psicométricos de consumo e direcionar anúncios com precisão cirúrgica baseada em dados pessoais (Zuboff, 2019), torna-se logicamente imperioso que apliquem esse mesmo nível de sofisticação para implementar filtros automatizados capazes de identificar assinaturas digitais (*hash matching*) de mídias sintéticas ilícitas.

Essa necessária mudança de paradigma operacional tem ganhado expressivo respaldo na jurisprudência e na atuação institucional do Estado brasileiro. O Superior Tribunal de Justiça (STJ), em precedente sob a relatoria da Ministra Nancy Andrighi, enfrentou a temática da inércia das plataformas digitais baseada em escusas de impossibilidade técnica e sigilo operacional (Brasil, 2025).

Na oportunidade, a Corte Superior assentou de forma categórica que o sigilo empresarial e as restrições tecnológicas de segurança não podem ser convertidos em um escudo genérico ou em um cheque em branco para a inércia das empresas, determinando que estas assumam a obrigação de adotar medidas de resultado prático equivalente para mitigar os danos suportados pelos usuários.

Em perfeita convergência, a atuação extrajudicial do Estado materializou essa imposição de um dever de cuidado proativo quando a Advocacia-Geral da União notificou provedores de busca para promover a imediata desindexação de sítios eletrônicos voltados à técnica de "*nudify*" (Brasil, 2026).

Amparada em relatórios que atestam a escala global da violência digital, a fundamentação estatal sustentou que os mecanismos de busca não podem se eximir de responsabilidade sob a alegação de não hospedarem diretamente os arquivos, haja vista que a indexação algorítmica potencializa o acesso em massa a ferramentas ilícitas.

Destarte, resta evidente que a tutela efetiva dos direitos existenciais na era da Inteligência Artificial exige a relativização do segredo industrial algorítmico, obstando que a opacidade corporativa atue como um salvo-conduto para a perpetuação de lesões permanentes à identidade e à dignidade dos cidadãos no ambiente virtual.

CONCLUSÃO

A análise dogmática, jurisprudencial e sociotécnica do fenômeno das mídias sintéticas revela que o enfrentamento da violência cibernética contemporânea não pode se restringir à persecução criminal ou à reparação civil tardia de seus criadores diretos. A mitigação efetiva do dano exige o combate estrutural à opacidade das corporações tecnológicas que arquitetam, hospedam e lucram com as vias de distribuição desses conteúdos.

Ficou demonstrado que o regime de responsabilidade civil edificado pelo Marco Civil da Internet (Brasil, 2014) encontra-se em estado de crônica defasagem frente ao atual estado da técnica algorítmica. A exigência de intervenção judicial prévia ditada pelo artigo 19 submete a integridade psíquica e moral dos indivíduos a um grau insuportável de vulnerabilidade, transformando a dilação processual no próprio vetor de agravamento e perpetuação do dano reputacional na rede (Pinheiro, 2021).

Mais gravosa, entretanto, é a constatação de que o sistema jurídico brasileiro legitima uma profunda inversão axiológica ao conferir proteção extrajudicial imediata a direitos patrimoniais e ativos corporativos da propriedade intelectual, enquanto relega a proteção dos atributos existenciais da personalidade humana aos entraves burocráticos do rito judicial ordinário (Schreiber, s.d.).

A pesquisa evidenciou a urgência em corrigir um modelo de tutela que age com celeridade para blindar direitos autorais das próprias plataformas, mas que subjuga a inviolabilidade da intimidade e da identidade digital do cidadão a limites operacionais de corporações. A invocação irrestrita da Lei nº 9.279/1996, especificamente o uso do "segredo de negócio" como escudo para ocultar a arquitetura falha dos algoritmos de moderação, opera como uma blindagem ilegítima (Brasil, 1996).

Essa retórica permite que as empresas de tecnologia recusem a implementação de filtros profiláticos automatizados e o bloqueio na origem (*hash matching*) de mídias sintéticas sob o falacioso argumento da proteção do capital informacional frente à livre concorrência (Pasquale, 2015).

Conclui-se, portanto, que a proteção constitucional da personalidade humana na era da Inteligência Artificial demanda a relativização procedimental e material dessa opacidade algorítmica. O ordenamento jurídico, iluminado pelas orientações consolidadas do Superior Tribunal de Justiça (Brasil, 2025) e pela atuação proativa de órgãos federais (Brasil, 2026), impõe às plataformas digitais um dever de cuidado dinâmico e proativo, compatível com o poder computacional que detêm.

A superação da violência cibernética não se concretiza por meio de reparações financeiras póstumas, mas sim pela interrupção preventiva e em tempo real das lesões na origem (Leonardi, 2005). Torna-se imperioso, destarte, afastar a propriedade industrial como escusa para a negligência técnica corporativa, garantindo, em caráter de primazia axiológica, o resgate do controle do indivíduo sobre sua própria imagem e identidade no ambiente virtual.

REFERÊNCIAS

AJDER, Henry *et al*. **The State of Deepfakes**: landscape, threats, and impact. Amsterdam: Deeptrace, 2019. Disponível em: https://enough.org/wp-content/uploads/2026/05/Deeptrace-the-State-of-Deepfakes-2019.pdf. Acesso em: 21 abr. 2026.

BRASIL. Advocacia-Geral da União. **AGU notifica Google para desindexar sites que criam nudes falsos com IA**. Brasília: AGU, 2026. Disponível em: https://www.gov.br/agu/pt-br/comunicacao/noticias/agu-notifica-google-para-desindexar-sites-que-criam-nudes-falsos-com-ia. Acesso em: 12 maio 2026.

BRASIL. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. **Código Penal**. Brasília, DF: Presidência da República, 1940. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 12 maio 2026.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil (Marco Civil da Internet). Brasília, DF: Presidência da República, 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 01 abr. 2026.

BRASIL. **Lei nº 9.279, de 14 de maio de 1996**. Regula direitos e obrigações relativos à propriedade industrial. Brasília, DF: Presidência da República, 1996. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9279.htm. Acesso em: 15 abr. 2026.

BRASIL. Superior Tribunal de Justiça. Recurso Especial nº 2.172.296/RJ. Relatora: Min. Nancy Andrighi. Terceira Turma. Julgado em 04 fev. 2025. **Diário da Justiça Eletrônico**, Brasília, DF, 07 fev. 2025.

BRASIL. Supremo Tribunal Federal. Recurso Extraordinário nº 1.057.258/MG. Tema 533 da Repercussão Geral. Relator: Min. Luiz Fux. Julgamento em 26 jun. 2025. **Portal do STF**, 2025. Disponível em: https://portal.stf.jus.br/jurisprudenciarepercussao/verAndamentoProcesso.asp?incidente=5217273&numeroProcesso=1057258&classeProcesso=RE&numeroTema=533. Acesso em: 11 abr. 2026.

DINIZ, Maria Helena. **Manual de direito civil**. 6. ed. São Paulo: Saraiva Jur, 2022. E-book.

KESAVARAJAH, Abiraam *et al*. **Deepfake technology unveiled**: the commoditization of AI and its impact on digital trust. [S. l.]: arXiv, 2025. Disponível em: https://arxiv.org/abs/2506.07363. Acesso em: 11 abr. 2026.

LEONARDI, Marcel. **Responsabilidade civil dos provedores de serviços de internet**. São Paulo: Juarez de Oliveira, 2005.

NAÇÕES UNIDAS. ONU Mulheres. **ONU alerta para aumento da violência digital contra mulheres e meninas impulsionada por inteligência artificial**. ONU News, mar. 2026. Disponível em: https://news.un.org/pt/story/2026/03/1852522. Acesso em: 16 abr. 2026.

PASQUALE, Frank. **The Black Box Society**: The Secret Algorithms That Control Money and Information. Cambridge: Harvard University Press, 2015.

PINHEIRO, Patricia Peck. **Direito digital**. 7. ed. São Paulo: Saraiva Educação, 2021. E-book.

RODRIGUES, Paulo Gustavo Lima e Silva. Deepfakes pornográficas não consensuais: a busca por um modelo de criminalização. **Revista Brasileira de Ciências Criminais**, São Paulo, v. 199, ano 31, p. 277-311, nov./dez. 2023. Disponível em: https://publicacoes.ibccrim.org.br/index.php/RBCCRIM/article/view/267/1008. Acesso em: 10 maio 2026.

SCHREIBER, Anderson. **Direitos da personalidade**. 2. ed. rev. e atual. São Paulo: Atlas, 2013.

SCHREIBER, Anderson. **Marco Civil da Internet**: avanço ou retrocesso? A responsabilidade civil por dano derivado do conteúdo gerado por terceiro. [s.d.]. Disponível em: https://www.academia.edu/28711449/Marco_Civil_da_Internet_Avan%C3%A7o_ou_Retrocesso. Acesso em: 23 abr. 2026.

ZUBOFF, Shoshana. **A era do capitalismo de vigilância**: a luta por um futuro humano na nova fronteira do poder. Rio de Janeiro: Intrínseca, 2019.