

**ÉTICA E SEGURANÇA PÚBLICA: DESAFIOS CONTEMPORÂNEOS NA ERA DAS
TECNOLOGIAS EMERGENTES**

**ETHICS AND PUBLIC SECURITY: CONTEMPORARY CHALLENGES IN THE ERA OF
EMERGING TECHNOLOGIES**

**ÉTICA Y SEGURIDAD PÚBLICA: DESAFÍOS CONTEMPORÂNEOS EN LA ERA DE LAS
TECNOLOGÍAS EMERGENTES**



10.56238/revgeov16n5-257

Wilson Garcia Pereira Junior

Doutorando em Engenharia e Tecnologia Ambiental

Instituição: Universidade Federal do Paraná

E-mail: garciaguibor@gmail.com

Lattes: <http://lattes.cnpq.br/1746884421002322>

Marta Helena Szadkoski

Doutoranda em Integração Contemporânea da América Latina

Instituição: Universidade Federal da Integração Latino-Americana

E-mail: m.h.szadkoski@gmail.com

Lattes: <http://lattes.cnpq.br/1034361124671052>

Juliana Helena Corrêa

Mestra em Integração Contemporânea da América Latina

Instituição: Universidade Federal da Integração Latino-Americana

E-mail: juhcl@yahoo.com.br

Lattes: <http://lattes.cnpq.br/2255518434587414>

Jocineia Medeiros

Doutoranda em Educação em Ciências e Educação Matemática

Instituição: Universidade Estadual do Oeste do Paraná

E-mail: jo4medeiros@gmail.com

Lattes: <https://lattes.cnpq.br/2701204991323650>

Adriano Krul Bini

Doutorando em Sociedade, Cultura e Fronteiras

Instituição: Universidade do Oeste do Paraná

E-mail: adriano16bini@gmail.com

Lattes: <http://lattes.cnpq.br/3667484790688530>



Aristides Samuel Machavane

Mestrando em Sociedade, Cultura e Fronteiras
Instituição: Universidade Estadual do Oeste do Paraná
E-mail: areitidesmachavane@gmail.com
Lattes: <http://lattes.cnpq.br/3081480171709098>

Aroldo da Silva Tavares

Mestre em Sociedade Cultura e Fronteiras
Instituição: Universidade Estadual do Oeste do Paraná
E-mail: professoraroldotavares@gmail.com
Lattes: <http://lattes.cnpq.br/6627759232681237>

Luciana Furlanetto Pereira

Doutoranda em Integração Contemporânea da América-Latina
Instituição: Universidade Federal da Integração da América-Latina
E-mail: lufurlanetto@gmail.com
Lattes: <http://lattes.cnpq.br/4359854623043927>

Luciane Cristina Silva

Doutora em Sociedade, Cultura e Fronteiras
Instituição: Universidade Estadual do Oeste do Paraná
E-mail: luciane_crisil@hotmail.com
Lattes: <http://lattes.cnpq.br/6168231813706604>

Marcos Galdino

Doutor em Sociedade, Cultura e Fronteiras
Instituição: Universidade Estadual do Oeste do Paraná
Lattes: <https://lattes.cnpq.br/0709004982508046>
E-mail: marcos.galdino@udc.edu.br

RESUMO

Os avanços das tecnologias digitais têm transformado profundamente as formas de interação humana, a dinâmica social e os mecanismos de cometimento de ilícitos, ampliando desafios éticos e riscos para a segurança pública. Se, há pouco mais de uma década, a expansão da internet já redefinía comportamentos e relações, hoje plataformas de redes sociais, o processamento massivo de dados e os sistemas de inteligência artificial intensificam tensões entre privacidade, liberdade e proteção coletiva. No Brasil, a promulgação do Marco Civil da Internet e da Lei Geral de Proteção de Dados estabeleceu novos parâmetros jurídicos para esse cenário, embora a velocidade das inovações tecnológicas frequentemente ultrapasse a capacidade normativa e institucional do Estado. Este artigo analisa, sob uma perspectiva crítica e interdisciplinar, como a evolução das tecnologias digitais desde 2010 reconfigurou valores éticos, práticas sociais e modalidades de crime, destacando: o papel dos algoritmos, da cultura do anonimato e da circulação de dados na amplificação de comportamentos antissociais; a maneira que tais transformações impactam a segurança pública; e quais são os desafios éticos emergentes para a sociedade contemporânea. Conclui-se que a consolidação de uma cultura digital responsável e alinhada a princípios éticos é condição indispensável para que a tecnologia



promova o bem-estar coletivo, e não se converta em um vetor de vulnerabilidade social capaz de pavimentar um ambiente propício para práticas criminosas.

Palavras-chave: Ética. Segurança Pública. Redes Sociais. Inteligência Artificial. Marco Civil da Internet. LGPD.

ABSTRACT

The rapid advancement of digital technologies has profoundly reshaped human interaction, social dynamics and the mechanisms by which illicit activities are carried out, generating new ethical challenges and increasing risks to public security. While the expansion of the internet had already redefined behaviors and relationships a little over a decade ago, today social media platforms, large-scale data processing and artificial intelligence systems intensify tensions among privacy, individual freedom and collective protection. In Brazil, the enactment of the Civil Rights Framework for the Internet (Marco Civil da Internet) and the General Data Protection Law (LGPD) established new legal parameters for addressing this scenario, although the speed of technological change often surpasses the normative and institutional capacity of the State. This article analyzes, from a critical and interdisciplinary perspective, how the evolution of digital technologies since 2010 has reconfigured ethical values, social practices, and forms of crime, highlighting: the role of algorithms, the culture of anonymity, and the circulation of data in amplifying antisocial behaviors; the way these transformations impact public safety; and the emerging ethical challenges for contemporary society. The article concludes that the consolidation of a responsible digital culture aligned with ethical principles is essential for ensuring that technology promotes collective well-being rather than becoming a vector of social vulnerability capable of fostering an environment conducive to criminal practices.

Keywords: Ethics. Public Safety. Social Networks. Artificial Intelligence. Brazilian Internet Bill of Rights. LGPD (Brazilian General Data Protection Law).

RESUMEN

Los avances en las tecnologías digitales han transformado profundamente las formas de interacción humana, las dinámicas sociales y los mecanismos para cometer delitos, amplificando los desafíos éticos y los riesgos para la seguridad pública. Si hace poco más de una década, la expansión de internet ya estaba redefiniendo comportamientos y relaciones, hoy las plataformas de redes sociales, el procesamiento masivo de datos y los sistemas de inteligencia artificial intensifican las tensiones entre la privacidad, la libertad y la protección colectiva. En Brasil, la promulgación del Marco Civil da Internet (Carta Brasileña de Derechos de Internet) y la Lei Geral de Proteção de Dados (Ley General de Protección de Datos Brasileña) establecieron nuevos parámetros legales para este escenario, aunque la velocidad de las innovaciones tecnológicas a menudo supera la capacidad normativa e institucional del Estado. Este artículo analiza, desde una perspectiva crítica e interdisciplinaria, cómo la evolución de las tecnologías digitales desde 2010 ha reconfigurado los valores éticos, las prácticas sociales y las formas de delincuencia, destacando: el papel de los algoritmos, la cultura del anonimato y la circulación de datos en la ampliación de los comportamientos antisociales; la forma en que estas transformaciones impactan en la seguridad pública; y los desafíos éticos emergentes para la sociedad contemporánea. Se concluye que la consolidación de una cultura digital responsable, alineada con los principios éticos, es condición indispensable para que la tecnología promueva el bienestar colectivo y no se convierta en un vector de vulnerabilidad social capaz de crear un entorno propicio para prácticas delictivas.

Palabras clave: Ética. Seguridad Pública. Redes Sociales. Inteligencia Artificial. Carta de Derechos de Internet de Brasil. LGPD (Ley General de Protección de Datos de Brasil).



1 INTRODUÇÃO

Nas últimas décadas, a sociedade testemunhou uma transformação profunda impulsionada pela digitalização das relações humanas, pela expansão das redes sociais e pela integração massiva de tecnologias de informação no cotidiano. O que inicialmente representava apenas a informatização de serviços e a facilitação da comunicação evoluiu para um ecossistema complexo, no qual dados, algoritmos e sistemas de inteligência artificial influenciam comportamentos individuais e coletivos, moldam percepções e produzem novas formas de interação social. Nesse cenário, práticas econômicas, culturais e políticas passaram a ocorrer de modo integrado às plataformas digitais, ao mesmo tempo em que emergem riscos inéditos à privacidade, à integridade informacional e à segurança pública.

A partir de 2010, a velocidade das inovações tecnológicas intensificou a convergência entre vida online e offline, ampliando a capacidade de vigilância, a circulação de dados pessoais e o impacto das interações mediadas por algoritmos. Redes sociais tornaram-se ambientes privilegiados para o compartilhamento de informações, formação de identidades, mobilização social e também para práticas ilícitas — do estelionato digital à disseminação de discursos de ódio, passando pela organização de crimes e pela manipulação psicológica em larga escala. A inteligência artificial, por sua vez, introduziu novos dilemas éticos por meio de sistemas de reconhecimento facial, decisões automatizadas, produção de conteúdos sintéticos (como deepfakes) e ferramentas de alto poder de influência social, muitas vezes operando como verdadeiras “caixas-pretas” de difícil auditabilidade (Tsamados, 2022).

No Brasil, o Estado buscou responder a essas transformações por meio de marcos regulatórios como o Marco Civil da Internet (Lei nº 12.965/2014) e a Lei Geral de Proteção de Dados (Lei nº 13.709/2018), que estabeleceram princípios e diretrizes para o uso da rede, proteção de dados pessoais e responsabilização de agentes públicos e privados. Apesar desses avanços, persistem desafios significativos: a assimetria entre a velocidade das mudanças tecnológicas e a capacidade normativa do país, a fragilidade institucional para lidar com crimes digitais, a dificuldade de fiscalização de práticas algorítmicas e a insuficiência de políticas públicas voltadas à educação digital e ao fortalecimento da cultura ética no ciberespaço (Damião, 2024).

Nesse contexto, discutir ética e segurança pública torna-se indispensável. O ambiente digital não apenas amplia oportunidades de desenvolvimento social e econômico, mas também intensifica vulnerabilidades e potencializa comportamentos antissociais, muitas vezes favorecidos pelo anonimato, pela desinformação e pela ausência de mecanismos de governança eficazes. Compreender como essas transformações alteram valores sociais, influenciam condutas e geram novas modalidades criminais é fundamental para o desenvolvimento de políticas públicas que conciliem liberdade, privacidade e proteção coletiva (Santos, 2017).



Diante desse panorama, este artigo busca analisar, sob uma perspectiva crítica e interdisciplinar, como a evolução das tecnologias digitais desde 2010 tem reconfigurado práticas sociais, valores éticos e dinâmicas de segurança pública no Brasil, procurando-se identificar os principais desafios éticos emergentes e refletir sobre caminhos possíveis para a construção de uma cultura digital responsável, capaz de mitigar riscos e fortalecer o bem-estar social.

Nesse cenário de reconfiguração ética, transformação tecnológica e fragilização dos mecanismos tradicionais de regulação e controle, emerge um problema central que orienta este estudo: **como a evolução das tecnologias digitais desde 2010 tem modificado comportamentos sociais, tensionado valores éticos e criado novas vulnerabilidades para a segurança pública no Brasil?** Embora haja vasta produção científica sobre internet, governança de dados e criminalidade digital, **a literatura nacional ainda carece de análises integradas** que articulem, de forma simultânea, ética aplicada, algoritmos, comportamento humano, anonimato, regulação estatal e práticas criminais emergentes. Essa lacuna teórico-analítica dificulta a compreensão sistêmica dos fenômenos contemporâneos que atravessam o ambiente digital e limita o desenvolvimento de políticas públicas mais eficazes.

Com isso, pretende-se oferecer uma síntese analítica capaz de contribuir para o debate acadêmico, preencher lacunas existentes e subsidiar reflexões sobre políticas públicas voltadas à construção de uma cultura digital mais ética, segura e socialmente responsável.

2 ÉTICA E MORAL

A Gestão do Conhecimento é vista como uma coleção de processos que governa a criação, disseminação e utilização do conhecimento para atingir plenamente os objetivos a que foram propostos (Jacomino, 2000). A Gestão do Conhecimento lida principalmente com aqueles aspectos críticos para a adaptação e sobrevivência das organizações, diante de um ambiente de mudança crescente e descontínuo.

Segundo Jacomino (2000), é no conhecimento coletivo que se baseiam as competências competitivas essenciais, e deve se ter limites bem definidos, pois a convivência em sociedade não permite que determinados grupos adotem uma postura individualista, devendo-se sempre pautar por princípios éticos e morais.

Mas afinal o que é Ética e Moral? A reflexão sobre ética e moral permanece central em sociedades atravessadas por transformações tecnológicas rápidas e por tensões entre liberdade individual, responsabilidade coletiva e segurança pública. Embora frequentemente utilizados como sinônimos, os termos possuem distinções conceituais relevantes que influenciam diretamente a interpretação das condutas humanas no ambiente digital e offline (Anchieta et al, 2022).



A ética, tradicionalmente compreendida como o campo filosófico que investiga os fundamentos das ações humanas, seus valores e finalidades, constitui um processo crítico e reflexivo que orienta a deliberação moral. Ética, portanto, não se confunde com um conjunto fixo de normas; trata-se de uma disciplina que problematiza e interpreta as práticas sociais à luz de valores como justiça, liberdade, dignidade e bem comum (Bauman, 2013). A ética se tornou ainda mais complexa diante da liquefação das relações humanas, da hipereposição digital e das dinâmicas algorítmicas que influenciam decisões e interações cotidianas.

Por sua vez, a moral refere-se ao conjunto de normas, valores e costumes historicamente constituídos e socialmente compartilhados por um grupo. Ela expressa prescrições de conduta — como “não prejudicar”, “não enganar”, “não violentar” — que orientam comportamentos coletivos e regulam expectativas sociais. A moral é histórica e mutável: evolui conforme as transformações culturais, econômicas e tecnológicas, refletindo as tensões e adaptações de cada sociedade (Schmitz, 2025). Assim, em contextos marcados pela digitalização, novas práticas morais emergem, enquanto outras são desafiadas pelos modos contemporâneos de comunicação e interação.

A distinção clássica entre ética e moral ajuda a compreender suas interdependências: enquanto a moral estabelece “o que é correto” dentro de uma sociedade, a ética pergunta *por que* algo deve ser considerado correto e *como* justificar racionalmente determinada conduta. Desse modo, a ética funciona como exame crítico da moral, permitindo revisá-la à medida que novas realidades sociais — como a economia digital, a vigilância por algoritmos, a circulação massiva de dados e os riscos de desinformação — colocam em xeque valores tradicionais (Santos, 2021).

No campo das organizações e políticas públicas, a relação entre ética, moral e gestão do conhecimento assume importância crescente. A literatura contemporânea reconhece que o conhecimento coletivo se tornou ativo estratégico, mas que seu uso deve ser orientado por princípios éticos sólidos, especialmente quando envolve dados sensíveis, tomada de decisões automatizadas ou impacto sobre direitos fundamentais (Floridi, 2013). A convivência em sociedade, sobretudo em regimes democráticos, não admite práticas individualistas ou instrumentalização do conhecimento para fins que violem a dignidade humana ou a integridade social.

Nesse sentido, a postura ética dos cidadãos, das instituições e do próprio Estado torna-se elemento determinante para a estabilidade e o bem-estar social. Em uma realidade marcada por desigualdades, discursos polarizados, dinâmicas de vigilância digital e potenciais abusos tecnológicos, agir eticamente significa não apenas evitar o dano, mas contribuir para a construção de um ambiente no qual a tecnologia sirva ao interesse público (Nunes e Lehfeld, 2019). Sociedades só se sustentam quando orientadas pela responsabilidade recíproca e pelo reconhecimento do outro como sujeito de direitos. Assim, ética e moral não são apenas categorias filosóficas abstratas, mas fundamentos concretos para enfrentar os dilemas do nosso tempo.



3 APLICAÇÃO ÉTICA NO CAMPO DAS NOVAS TECNOLOGIAS

A incorporação acelerada de tecnologias digitais às atividades econômicas, políticas e sociais ampliou significativamente os desafios éticos que permeiam organizações públicas e privadas. Embora se fale frequentemente em “empresas éticas”, é importante reconhecer que nenhuma instituição possui moral própria; a ética manifesta-se nas decisões de indivíduos reais — dirigentes, gestores, técnicos e colaboradores — que atuam em múltiplos níveis. Assim, decisões equivocadas, omissões ou práticas negligentes não são falhas abstratas, mas resultados de escolhas humanas que repercutem diretamente na credibilidade, na imagem e na sustentabilidade institucional. O ecossistema digital amplia tanto o poder das corporações quanto o impacto ético de suas ações, fazendo com que cada decisão tecnológica carregue implicações sociais de grande escala (Tsamados, 2022).

A cultura contemporânea, marcada pela hiperconsumação, pela lógica da performance e pela economia da atenção, tende a deslocar valores éticos para segundo plano. O ambiente digital não apenas facilita comportamentos consumistas, mas os estimula continuamente por meio de algoritmos orientados a maximizar engajamento e lucro. O capitalismo de vigilância transformou a coleta e exploração de dados pessoais em uma mecânica de lucro, moldando comportamentos, preferências e emoções em tempo real. Nesse cenário, o desejo de aquisição permanente, já presente antes da era digital, tornou-se mais intenso, imediato e automatizado — e, para muitos, quase inevitável (Arnd-Caddigan e Turkle, 2015).

Com o comércio eletrônico, a publicidade personalizada, os sistemas de recomendação e a economia de plataformas, o usuário é constantemente exposto a estímulos que encorajam decisões impulsivas, consumo irracional e adesão a tendências massificadas. Ao mesmo tempo, estruturas simbólicas tradicionais — que antes funcionavam como referências éticas, comunitárias ou institucionais — são substituídas por lógicas de visibilidade, aprovação instantânea e recompensas rápidas, características das redes sociais digitais. Essas dinâmicas produzem um ambiente culturalmente propenso à superficialidade e à perda de profundidade ética nas relações humanas (Môcho, 2025).

Nesse contexto, o campo das novas tecnologias torna-se um dos espaços mais carentes de uma reflexão ética consistente. Não apenas porque as transformações são rápidas demais para que a legislação acompanhe, mas porque muitos profissionais atuam em áreas cuja normatividade ainda é incipiente, como inteligência artificial, análise massiva de dados, vigilância digital, machine learning e automação de decisões. Paradoxalmente, quanto mais sofisticadas as tecnologias, maior a necessidade de responsabilidade humana na definição de limites, parâmetros e finalidades (Prado, 2025).

A ausência de regulamentação específica para diversas práticas, aliada à opacidade algorítmica e ao anonimato facilitado nas plataformas digitais, dificulta o estabelecimento de fronteiras claras entre



condutas aceitáveis e violações éticas. É nesse vácuo que se multiplicam usos oportunistas da tecnologia, afetando tanto usuários vulneráveis quanto instituições que dependem da confiança pública (Marques, 2022). A legislação busca estabelecer salvaguardas — como ocorre com a LGPD —, mas ainda há um descompasso entre a proteção jurídica e a realidade concreta das práticas digitais, permitindo que atores mal-intencionados explorem brechas com relativa facilidade.

A ética, portanto, não deve ser vista apenas como uma área teórica de reflexão, mas como um **investimento estratégico**. Organizações que incorporam princípios éticos desde a concepção de produtos e serviços digitais tendem a mitigar riscos legais, fortalecer reputação, melhorar relações com stakeholders e contribuir para um ambiente digital mais seguro e confiável. Práticas éticas em tecnologia — especialmente em IA — não são apenas uma exigência moral, mas um fundamento para inovação sustentável, legitimidade social e proteção da dignidade humana (Mittelstadt, 2019; Morley et al., 2021).

A aplicação ética no campo das novas tecnologias exige mais do que conformidade normativa: implica reconhecer a responsabilidade humana por trás das decisões técnicas e compreender que cada linha de código, cada coleta de dados e cada decisão automatizada pode gerar efeitos profundos sobre indivíduos e sociedades.

4 MARCO LEGAL BRASILEIRO SOBRE TECNOLOGIAS DIGITAIS E SEGURANÇA PÚBLICA

A construção do marco regulatório brasileiro para o ambiente digital é relativamente recente e ainda marcada por tensões entre proteção de direitos fundamentais, responsabilidade das plataformas e necessidade de enfrentamento dos ilícitos que se multiplicam no ciberespaço. O Marco Civil da Internet, promulgado em 2014, representou um avanço ao estabelecer princípios como neutralidade da rede, proteção à privacidade e responsabilização condicionada dos provedores de aplicações. Entretanto, ao priorizar um modelo de garantias amplas e de responsabilização apenas após ordem judicial específica, criou-se um sistema que, embora fundamental para evitar censura privada e abusos estatais, também produz limitações práticas quando se trata de respostas rápidas a conteúdos ilícitos, discursos de ódio, fraudes e ataques coordenados que se proliferam em velocidade incompatível com os tempos processuais (Bispo et al, 2023).

O modelo brasileiro, ao proteger com rigor a liberdade de expressão e ao impor barreiras significativas para responsabilização imediata de intermediários, acaba oferecendo um terreno fértil para que indivíduos mal-intencionados explorem brechas, valendo-se do anonimato, da volatilidade das contas e da arquitetura algorítmica das plataformas. Embora essa não seja a intenção do legislador, na prática há uma assimetria: cidadãos que atuam de boa-fé dependem da morosidade judicial para ver seus direitos resguardados, enquanto oportunistas digitais se aproveitam do vácuo temporal para



disseminar ataques, enganos, extorsões e manipulação social. Trata-se de uma crítica que emerge não como condenação ao marco legal, mas como constatação de que a velocidade dos crimes digitais supera a capacidade de reação das instituições — e isso exige reflexão constante (Carneiro et al, 2022).

A Lei Geral de Proteção de Dados (LGPD), por sua vez, introduziu no Brasil parâmetros modernos de governança e tratamento de dados pessoais, reforçando princípios de finalidade, necessidade e transparência. Foi um avanço importante para garantir que empresas e órgãos públicos adotem critérios mais rígidos no tratamento de informações, especialmente em um contexto de crescente uso de inteligência artificial, reconhecimento facial e tomada de decisões automatizadas. Contudo, assim como ocorre com o Marco Civil, a LGPD enfrenta desafios diante das novas dinâmicas tecnológicas. O tratamento de dados em escala massiva, muitas vezes por atores transnacionais, cria zonas de difícil fiscalização. A própria Autoridade Nacional de Proteção de Dados (ANPD), ainda em consolidação institucional, encontra limites para monitorar um ecossistema vasto e em mutação acelerada (Bispo et al, 2023).

Embora a LGPD seja um marco de proteção de direitos, sua aplicação no cotidiano revela tensões entre segurança pública, privacidade e responsabilização. A proteção rigorosa dos dados pode, em certos casos, dificultar investigações quando não há clareza sobre bases legais aplicáveis ou quando há receio de violações interpretativas. Mais uma vez, a intenção do legislador é justa e necessária, mas o ambiente digital, ao permitir anonimato sofisticado, perfis falsos e manipulação de identidades, acaba oferecendo a criminosos um abrigo regulatório que cidadãos comuns não possuem (Bispo et al, 2023). Assim, não é exagero reconhecer que a legislação, tal como se encontra, protege de forma desigual: quem age de boa-fé fica exposto; quem atua no limite da ilegalidade explora as entrelinhas.

O direito penal brasileiro também buscou, ao longo da última década, responder ao surgimento de crimes digitais. A chamada “Lei Carolina Dieckmann” e alterações posteriores endureceram penas para invasões, fraudes eletrônicas e manipulações de dados. Ainda assim, os delitos contemporâneos — deepfakes maliciosos, ataques automatizados, golpes orquestrados por redes transnacionais, engenharia social avançada — evidenciam que o arsenal jurídico ainda é insuficiente. Não se trata apenas de ausência normativa, mas de uma mudança estrutural na lógica da criminalidade: o custo da prática delitiva diminuiu, o anonimato aumentou e a capacidade de dano se ampliou de forma exponencial (Bispo et al, 2023).

O Marco Legal Brasileiro avançou, mas permanece tensionado entre a defesa das liberdades e a necessidade de proteção da sociedade. É um arcabouço que, embora bem-intencionado e fundamental para preservar direitos, mostra-se parcial e limitado diante da complexidade das interações digitais. Não por falha intrínseca, mas porque o ambiente tecnológico atual desafia categorias tradicionais do direito (Carneiro et al, 2022). Isso exige não apenas atualização normativa, mas também políticas públicas, educação digital e mecanismos institucionais capazes de equilibrar liberdades individuais e



segurança coletiva, reduzindo o espaço de ação daqueles que se aproveitam da arquitetura da internet para práticas reprováveis ou criminosas.

5 A INFLUÊNCIA DA INTERNET NA SOCIEDADE CONTEMPORÂNEA

A expansão da internet, nas últimas décadas, transformou de maneira profunda a experiência humana, afetando hábitos de leitura, dinâmicas econômicas, relações interpessoais e a própria estrutura social. Nunca houve na história um meio de comunicação que se difundisse tão rapidamente e com tamanha capacidade de reorganizar comportamentos, instituições e práticas culturais. Ao mesmo tempo, a lógica de acesso, produção e circulação de informação tornou-se desigual, revelando profundas assimetrias entre grupos, regiões e classes sociais — um dos traços mais marcantes da sociedade digital contemporânea (Prado, 2025).

A abundância de informação, celebrada como uma conquista da era digital, traz consigo ambivalências. Embora facilite o acesso ao conhecimento e amplie possibilidades de aprendizagem, também intensifica riscos associados à desinformação, ao consumo superficial de conteúdo e à dificuldade crescente de selecionar informações confiáveis. A internet não é apenas uma tecnologia neutra: ela estrutura modos de ver o mundo, cria padrões de relevância e redefine a própria materialidade das interações sociais.

5.1 INTERNET E TRANSFORMAÇÕES CULTURAIS

A leitura — atividade central para o desenvolvimento crítico, cognitivo e simbólico — sofreu impacto direto das novas tecnologias. O consumo de textos fragmentados, hiperlinks, estímulos rápidos e interfaces visuais alterou padrões de atenção, reduzindo a profundidade da leitura tradicional. O fluxo contínuo de informações digitais cria um ambiente que privilegia rapidez em detrimento da reflexão, tornando mais difícil sustentar atenção prolongada e engajar-se em conteúdos complexos (Tamandaré, 2025).

Ao mesmo tempo, o ambiente escolar e as bibliotecas passaram a competir com dispositivos digitais que oferecem, simultaneamente, entretenimento, comunicação e acesso imediato a múltiplas fontes de informação. Isso desloca a função mediadora da escola e exige novas estratégias pedagógicas que fomentem leitura crítica, interpretação e autonomia intelectual.

5.2 INTERNET E ECONOMIA DIGITAL

No campo econômico, a internet alterou radicalmente a lógica do consumo. A emergência do comércio eletrônico, aliada à economia de plataformas, mecanismos de comparação de preços e publicidade comportamental, redefiniu a experiência de compra. O consumidor passou a ter acesso imediato a produtos, avaliações, recomendações e alternativas globais. Essa reconfiguração reduziu



assimetrias de mercado, mas também incentivou práticas consumistas intensas (**Nonaka e Takeuchi, 2019**).

Plataformas digitais operam com modelos de negócio baseados na extração e monetização de dados comportamentais, influenciando decisões de compra e moldando preferências individuais. O resultado é um ecossistema econômico que combina conveniência com vigilância, personalização com persuasão, autonomia com manipulação subliminar (Môcho, 2025).

A ascensão das empresas “ponto-com”, ainda no final do século XX, simbolizou essa nova economia, que continua se expandindo com o uso de inteligência artificial em marketing, análises preditivas e otimização de comportamento do consumidor.

5.3 INTERNET E RELAÇÕES HUMANAS

As formas tradicionais de sociabilidade também foram profundamente reconfiguradas. A internet criou um novo espaço de interação no qual identidade, presença e vínculo passaram a operar segundo lógicas distintas da convivência física. Relações mediadas por telas misturam intimidade e distância, autenticidade e performance, proximidade emocional e desconexão afetiva (Arnd-Caddigan e Turkle, 2015).

O anonimato — parcial ou completo — tornou-se elemento central dessas interações. Ele permite experimentações identitárias legítimas, mas também favorece comportamentos oportunistas, manipulação emocional e práticas antiéticas. A criação de avatares, perfis fictícios e identidades idealizadas abre espaço para novas possibilidades de expressão, porém amplia riscos de enganos, fraudes afetivas e vínculos assimétricos.

A busca por relações virtuais, frequentemente marcada por idealização e projeção de expectativas, pode gerar frustrações significativas. O sujeito cria uma narrativa de si mesmo e do outro que, ao colidir com a realidade, pode desencadear desilusão, instabilidade emocional e isolamento. Estudos em psicologia digital indicam que essa dinâmica não decorre apenas de escolhas individuais, mas da própria arquitetura das plataformas, que priorizam gratificação rápida, visibilidade e estímulos contínuos (Silva Barbosa, 2014).

5.4 REDES SOCIAIS

As redes sociais tornaram-se, possivelmente, o ambiente de maior impacto na forma como indivíduos constroem identidades e percebem o mundo. Elas reconfiguram a noção de comunidade, transformam a visibilidade em capital simbólico e intensificam a lógica da comparação constante (Vermelho, 2015; Carr, 2020).

O problema central não está apenas na existência das redes, mas em sua **arquitetura algorítmica**, que privilegia conteúdo emocionalmente carregado, polarizador e altamente



compartilhável. Esse mecanismo molda debates públicos, reforça bolhas informacionais e tende a amplificar comportamentos antiéticos — como ataques anônimos, assédio, manipulação emocional e disseminação de desinformação.

O sujeito, orientado a performar para manter relevância e aceitação, desenvolve relações mediadas por expectativas irreais, o que fragiliza vínculos reais e pode acentuar sentimentos de inadequação e solidão. Em paralelo, criminosos exploram essas fragilidades, utilizando perfis falsos, engenharia social e manipulação para fraudes, extorsão e outras práticas ilícitas (Vermelho, 2015).

5.5 ALGORITMOS E INTELIGÊNCIA ARTIFICIAL

A influência da internet na sociedade contemporânea não pode ser compreendida sem considerar o papel dos algoritmos e da inteligência artificial (IA). Essas tecnologias atuam como “filtros invisíveis” que definem o que vemos, consumimos e acreditamos. Algoritmos opacos podem reforçar desigualdades, enviesar decisões e manipular percepções de modo imperceptível ao usuário (Kaufman, 2020).

Com a expansão da IA generativa, sistemas de recomendação, reconhecimento facial e decisões automatizadas, cresce a tensão entre conveniência e vigilância, eficiência e discriminação, liberdade e controle. A lógica algorítmica, ao priorizar previsibilidade e padrões estatísticos, pode empobrecer a complexidade humana e estimular comportamentos padronizados, reproduzindo vieses em escala industrial.

Além disso, tecnologias avançadas ampliam a capacidade de criminosos explorarem brechas: deepfakes, perfis sintéticos, golpes automatizados e manipulação psicológica sofisticada compõem um novo ecossistema de riscos éticos e de segurança pública (Kaufman, 2020).

6 AVANÇOS TECNOLÓGICOS E SEGURANÇA PÚBLICA

A sociedade contemporânea experimenta uma transformação acelerada impulsionada por tecnologias digitais que reconfiguram comportamentos, instituições e estruturas sociais. Ignorar essa mudança — ou responder a ela de forma lenta e desarticulada — significa permitir que lacunas normativas, fragilidades éticas e vulnerabilidades tecnológicas criem terreno fértil para novas modalidades de condutas antissociais e práticas criminosas (Kaufman, 2020). A relação entre tecnologia e segurança pública, portanto, é inevitavelmente tensa: ao mesmo tempo em que a inovação oferece ferramentas de proteção, transparência e eficiência, ela também amplia oportunidades para crimes sofisticados e dificulta a atuação das autoridades.

A característica mais marcante da sociedade atual é justamente sua crescente **dependência de infraestruturas digitais**, que moldam desde as relações pessoais até o funcionamento do Estado. As tecnologias da informação não apenas alteram rotinas e modelos de trabalho, mas influenciam valores,



percepções e expectativas sociais, criando uma realidade em que a vida online se confunde com a offline. Vivemos em uma “sociedade em rede” na qual a lógica dos fluxos informacionais se sobrepõe à lógica tradicional das instituições (Prado, 2025).

Entretanto, esse avanço tecnológico nem sempre é acompanhado pela capacidade do Estado em atualizar suas estruturas legais e operacionais. O Código Penal Brasileiro, elaborado na década de 1940, jamais poderia prever delitos relacionados a ransomware, engenharia social, vazamento massivo de dados, deepfakes ou manipulação algorítmica. Apesar de reformas pontuais — como a “Lei Carolina Dieckmann” e o endurecimento das penas para fraudes digitais — permanece evidente uma **assimetria entre a complexidade dos crimes cibernéticos e a resposta estatal**, frequentemente lenta e insuficiente. A literatura contemporânea ressalta que essa defasagem normativa cria espaços de impunidade explorados por agentes mal-intencionados (Carneiro et al, 2022).

Além dos crimes tradicionais reconfigurados pelo ambiente digital — fraudes bancárias, pedofilia, invasões de sistema — surgem crimes baseados na **extração e manipulação de dados públicos**. Perfis em redes sociais, bases abertas e plataformas digitais fornecem informações detalhadas que podem ser utilizadas para golpes, extorsões, estelionato emocional, perseguições e até crimes violentos. A facilidade de disseminação de ideologias extremistas ou discursos de ódio também desempenha papel significativo na radicalização de indivíduos, conforme demonstram estudos sobre violência mediada pela rede (Yasin, 2017).

A internet ampliou não apenas o acesso à informação lícita, mas também a conteúdos ilícitos que ensinam a fabricar artefatos explosivos, realizar golpes digitais ou manipular pessoas. O ciberespaço funciona simultaneamente como espaço de inovação e espaço de risco, no qual a ausência de barreiras físicas reduz custos e amplia alcance de comportamentos de alta periculosidade (Carneiro et al, 2022).

Nesse contexto, a discussão sobre segurança pública não se resume à criação de novos tipos penais, mas à necessidade de um modelo regulatório capaz de equilibrar liberdade, proteção de dados e responsabilização. Uma legislação excessivamente rígida pode violar direitos fundamentais; uma legislação permissiva demais pode transformar a internet em um ambiente de impunidade. O desafio consiste em construir um sistema jurídico adaptável, que combata práticas criminosas sem sacrificar garantias democráticas — um equilíbrio difícil em tempos de alta complexidade informacional (Siqueira e Nunes, 2018).

A atuação estatal, no entanto, deve ir além do direito penal. Políticas de educação digital, ética tecnológica e cidadania informacional são essenciais para evitar que indivíduos se tornem apenas “números” em um ecossistema digital dominado por interesses econômicos, algoritmos opacos e disputas simbólicas. A fragilização das relações interpessoais, intensificada pela mediação digital,



tende a enfraquecer o sentido de coletividade e preparar terreno para crises sociais mais amplas, como demonstram pesquisas sobre tecnossociabilidade contemporânea (Silva Barbosa, 2014).

A segurança pública está intimamente ligada à forma como a sociedade utiliza as tecnologias. Em um mundo onde informações circulam em tempo real, a manipulação de dados — seja por campanhas coordenadas de desinformação, seja por grupos organizados com interesses escusos — pode gerar colapsos locais, pânico social e reações coletivas desproporcionais. Sem um uso ético da informação e sem estruturas institucionais capazes de responder com celeridade e precisão, o risco de desordem cresce significativamente.

Ao discutir a necessidade de uma legislação capaz de acompanhar as demandas crescentes da sociedade digital, é necessário esclarecer que isso não implica transformar o aparato jurídico em ferramenta ideológica ou de repressão a opiniões divergentes. A construção normativa deve evitar qualquer desvio que permita ao Estado agir seletivamente contra discursos críticos ou contramajoritários, pois tal prática comprometeria princípios democráticos essenciais, como liberdade de expressão, pluralidade e controle social do poder. O objetivo é estabelecer mecanismos transparentes, verificáveis e impessoais, que delimitem objetivamente quais condutas configuram riscos reais à integridade ética do ambiente digital — tais como fraude, manipulação algorítmica, extorsão, desinformação maliciosa, discriminação, violação de dados e práticas que atentem contra a segurança pública. Uma legislação sólida não se mede pela sua capacidade de silenciar vozes discordantes, mas pela sua habilidade de proteger direitos, garantir segurança e promover um ambiente digital confiável e justo.

Para alcançar esse equilíbrio, propõe-se uma solução baseada na governança algorítmica multissetorial, que integre Estado, universidades, especialistas independentes, setor privado e sociedade civil. Em vez de decisões concentradas e subjetivas, este modelo pressupõe comissões técnicas permanentes, com representação diversa, responsáveis por avaliar riscos, revisar protocolos, auditar algoritmos, propor medidas regulatórias e monitorar abusos estatais ou corporativos.

Tais instâncias devem possuir critérios públicos, métricas claras e relatórios obrigatórios, de modo que qualquer intervenção estatal — seja para retirar conteúdo, investigar ilícitos ou restringir práticas abusivas — fique registrada, justificada e sujeita a escrutínio social e jurídico. Dessa forma, cria-se um ecossistema regulatório capaz de combater condutas antiéticas e criminosas sem abrir espaço para perseguições políticas, fortalecendo simultaneamente a segurança digital, a ética pública e a confiança institucional (Holt et al, 2022).

Assim, a construção de uma sociedade segura na era digital não depende exclusivamente do aparato policial ou jurídico, mas da combinação entre **ética, responsabilização, educação, governança algorítmica e modernização institucional**. A tecnologia continuará avançando; a



questão central é se a sociedade e o Estado conseguirão acompanhá-la com a mesma velocidade — ou se continuarão reagindo tardiamente aos danos.

7 SEGURANÇA PÚBLICA NA ERA DIGITAL

A análise integrada da literatura contemporânea, do arcabouço legal brasileiro e das dinâmicas sociais mediadas por tecnologias digitais revela um cenário complexo, no qual avanços tecnológicos convivem simultaneamente com vulnerabilidades estruturais. Os resultados da revisão bibliográfica indicam que o ambiente digital ampliou oportunidades para inovação, eficiência e democratização da informação, mas também criou vetores capazes de intensificar desigualdades, vulnerabilizar cidadãos e desafiar profundamente o sistema de segurança pública (Damião, 2024).

Um dos primeiros resultados observados diz respeito ao desequilíbrio entre o ritmo acelerado da inovação tecnológica e a capacidade de resposta do Estado. Estudos recentes demonstram que a legislação brasileira, embora tenha avançado com o Marco Civil da Internet e a LGPD, permanece insuficiente para lidar com fenômenos contemporâneos como desinformação algorítmica, deepfakes, crimes cibernéticos transnacionais e vazamentos massivos de dados. Esse hiato normativo é interpretado pela literatura como um dos principais fatores que sustentam a sensação de “terra sem lei” no ambiente digital, gerando terreno fértil para oportunistas explorarem brechas regulatórias (Damião, 2024).

Outro achado relevante diz respeito ao impacto das redes sociais como aceleradores comportamentais. As plataformas não apenas permitem a comunicação instantânea, mas também operam com algoritmos que amplificam conteúdos emocionalmente carregados — muitas vezes sensacionalistas, distorcidos ou até criminosos. A radicalização digital, o discurso de ódio e o aliciamento para práticas ilícitas aparecem de forma recorrente em estudos recentes, fortalecendo compreensões de que a tecnologia não é neutra, mas estruturante de comportamentos coletivos. Assim, a segurança pública passa a depender não só da repressão estatal, mas também de mecanismos de governança tecnológica capazes de conter danos antes que se tornem incontroláveis (Holt et al, 2022).

Resultados específicos também emergem no campo da vulnerabilidade individual. A exposição voluntária de dados nas redes sociais, aliada à coleta invisível e contínua de informações por grandes plataformas, cria um perfil digital detalhado que pode ser explorado para golpes, extorsões, perseguições ou manipulação. A imprevisibilidade do comportamento humano diante dessas ferramentas, aliada à assimetria de informação entre usuários e corporações, acentua o desafio: a segurança torna-se não apenas uma questão técnica, mas também ética e educacional (Nunes e Lehfeld, 2019).

A discussão também evidencia que a criminalidade digital não se limita a práticas sofisticadas. Em muitos casos, condutas aparentemente banais — como a replicação irrefletida de conteúdos, o



compartilhamento de informações sensíveis, ou o engajamento em discursos polarizados — reforçam ecossistemas nocivos que podem gerar violência no mundo físico. A fronteira entre o digital e o real torna-se difusa, e o dano informacional passa a ter materialidade concreta.

Outro ponto crítico observado é a tensão entre liberdade e controle. A literatura demonstra que um Estado excessivamente intervencionista pode comprometer garantias fundamentais; por outro lado, um Estado permissivo demais favorece a impunidade digital. O equilíbrio exige maturidade institucional e participação social, além de políticas públicas que envolvam educação digital, transparência algorítmica, fortalecimento das capacidades investigativas e atualização contínua das normas existentes. Não se trata de criar leis infinitas, mas de aplicar de forma eficaz as leis que já existem, complementadas por ajustes técnicos alinhados à evolução tecnológica (Damião, 2024).

A expansão acelerada dos crimes digitais expõe também, com clareza crescente um dos pontos mais relevantes para a percepção de um ambiente de impunidade digital, a total e absoluta incapacidade técnica do Estado em acompanhar a complexidade das infraestruturas sociotecnológicas contemporâneas. Órgãos de segurança, Ministério Público e sistemas judiciários continuam operando majoritariamente com métodos analógicos, enquanto criminosos exploram anonimização, redes descentralizadas, criptografia avançada, IA generativa e plataformas transnacionais. Essa assimetria tecnológica cria um ambiente de impunidade estrutural, no qual o Estado reage apenas depois do dano consolidado — e muitas vezes sem a capacidade de rastrear autoria, reconstruir cadeias de evidências ou compreender o funcionamento dos próprios sistemas que busca regular. Sem domínio mínimo dessas tecnologias, torna-se inviável identificar padrões de comportamento, mapear fluxos de informação ilícita ou antecipar riscos emergentes, o que reforça a percepção social de fragilidade institucional diante do crime digital (Santos, 2021).

Soma-se a isso a crônica falta de investimento contínuo em tecnologia, infraestrutura e capacitação pessoal, que compromete drasticamente a eficácia das ações de segurança pública no ambiente digital. Delegacias especializadas operam com equipes reduzidas, ferramentas defasadas e formação técnica insuficiente para lidar com algoritmos de ocultação, engenharia social avançada, fraudes massificadas ou manipulações algorítmicas complexas. A ausência de programas robustos de treinamento, atualização profissional e cooperação internacional limita a capacidade investigativa e aumenta a dependência de iniciativas externas, muitas vezes voluntárias, para solucionar incidentes de grande impacto social. A superação desse cenário exige que o Estado trate o combate ao crime digital como política de Estado e não como ação pontual, com investimentos estruturantes em centros de inteligência, laboratórios forenses digitais, plataformas de monitoramento ético e formação continuada, assegurando que a proteção da sociedade acompanhe a velocidade da transformação tecnológica (Nunes e Lehfeld, 2019).



Por fim, os resultados apontam para a necessidade de uma ética digital robusta, capaz de orientar empresas, governos e cidadãos a respeito do uso responsável de tecnologias. A revisão realizada evidencia que a erosão dos valores coletivos — intensificada pelo imediatismo das conexões e pela cultura da performance — fragiliza o senso de pertencimento e dificulta a cooperação, elementos fundamentais para qualquer estratégia de segurança pública. A tecnologia, portanto, não é o problema em si, mas um catalisador que pode potencializar tanto o bem quanto o mal, dependendo do modo como é governada (**Holt et al, 2022**).

Diante desse panorama, conclui-se que a segurança pública na era digital depende de uma combinação de fatores: modernização institucional, alfabetização digital da população, responsabilização dos agentes tecnológicos, e uma compreensão ética que reconheça a centralidade do ser humano diante dos algoritmos. A tecnologia continuará avançando; o desafio reside em garantir que seus benefícios superem seus riscos.

8 CONCLUSÃO

O cenário que se delineia no século XXI revela uma configuração social profundamente distinta daquela experimentada em gerações anteriores. A expansão da teleinformática, dos dispositivos pessoais e da circulação massiva de dados tornou o indivíduo mais autônomo, mais conectado e, ao mesmo tempo, paradoxalmente mais vulnerável. Contudo, essa autonomia tecnológica não foi acompanhada, na mesma intensidade, por um fortalecimento ético e social; pelo contrário, observa-se um enfraquecimento progressivo de valores coletivos, agravado por um ambiente digital onde o anonimato fragmenta identidades e reduz pessoas a logins, perfis ou avatares.

Inseridos nessa transformação vertiginosa, torna-se difícil antecipar todas as consequências do fenômeno a longo prazo. Ainda assim, é possível identificar tendências nítidas: comportamentos mais individualizados, níveis crescentes de criticidade seletiva, independência opinativa marcada por bolhas informacionais e um afastamento do sentimento de pertencimento coletivo. Esses fatores, somados à ausência de mecanismos eficazes de regulação do ciberespaço, contribuem para o surgimento de uma nova classe de problemas sociais e criminais, diretamente relacionados à fragilização dos laços comunitários e à expansão de práticas prejudiciais sob a proteção do anonimato.

Há, portanto, um descompasso entre as possibilidades proporcionadas pela tecnologia e a capacidade ética da sociedade para utilizá-las de forma responsável. A modernidade, ao reforçar uma cultura do “ter” em detrimento do “ser”, produz distorções que reverberam no tecido social — da radicalização digital ao consumo desenfreado, da desinformação à instrumentalização da tecnologia por grupos oportunistas. O Estado, cuja função primária deveria ser a regulação justa e isenta, muitas vezes encontra-se deslocado, por vezes alinhado a interesses corporativos que acentuam desigualdades e fragilizam a segurança pública.



Compreender as revoluções tecnológicas e seus impactos sobre o funcionamento do Estado é fundamental para analisar criticamente o papel da informática na sociedade contemporânea. O futuro próximo tende a ser marcado por maior participação dos indivíduos nos processos decisórios, estimulada pela democratização do acesso à informação. No entanto, essa participação só será socialmente benéfica se acompanhada por uma maturidade ética capaz de orientar decisões e ações para além do interesse individual.

Assim, a consolidação de uma sociedade equilibrada, segura e inclusiva dependerá da capacidade de formar cidadãos — e gestores públicos — plenamente conscientes das implicações sociais do ambiente digital. A tecnologia, por si só, não determinará o rumo da civilização; serão as escolhas éticas daqueles que a desenvolvem, regulam e utilizam que definirão se caminharemos para uma sociedade mais justa e colaborativa ou para um ambiente ainda mais fragmentado e instável. O desafio está colocado, e seu enfrentamento exige responsabilidade, visão crítica e compromisso coletivo.



REFERÊNCIAS

ANCHIETA, G. O. S., CARVALHO, A. S. M., ALBUQUERQUE, L. F. S., SOUTO, P. F., SILVA, L. C. A., & ARAUJO, P. Q. (2022). Diferenças entre Ética e Moral. *E-Acadêmica*, 3(1), e053183. <https://doi.org/10.52076/eacad-v3i1.83>

ARND-CADDIGAN, M. Sherry TURKLE: Alone Together: Why We Expect More from Technology and Less from Each Other. *Clin Soc Work J* 43, 247–248 (2015). <https://doi.org/10.1007/s10615-014-0511-4>

BAUMAN, Zygmunt. Danos colaterais: desigualdades sociais numa era global. Editora Schwarcz-Companhia das Letras, 2013.

BISPO, Adrielle da Silva; BINTO, Emanuel Vieira. Crimes cibernéticos: da ineficácia da lei carolina dieckmann na prática de crimes virtuais. *Revista Ibero-Americana de Humanidades, Ciências e Educação*, [S. l.], v. 9, n. 11, p. 354–369, 2023. DOI: <https://doi.org/10.51891/rease.v9i11.12291>

CARNEIRO, L. V. V.; SANTOS, J. N.; EDLER, G. O. B. Direito cibernético: o impacto gerado pela lei carolina dieckmann no combate aos crimes virtuais realizados contra as crianças e adolescentes. *Revista Ibero-Americana de Humanidades, Ciências e Educação*, [S. l.], v. 8, n. 11, p. 2061–2080, 2022. DOI: <https://doi.org/10.51891/rease.v8i11.7793>

CARR, Nicholas. The shallows: What the Internet is doing to our brains. WW Norton & Company, 2020.

DAMIÃO, A. S., & Novais, T. G. (2024). Consequências jurídicas da lgpd para os crimes virtuais. *Revista Ibero-Americana De Humanidades, Ciências E Educação*, 10(11), 6590–6613. <https://doi.org/10.51891/rease.v10i11.17054>

YASIN, N. A. M. “The Evolution of Online Extremism in Malaysia.” *Counter Terrorist Trends and Analyses* 9, no. 7 (2017). DOI: <http://www.jstor.org/stable/26351534>

FLORIDI, L. The Ethics of Information. Oxford: Oxford University Press, 2013. DOI: <https://doi.org/10.1093/acprof:oso/9780199641321.001.0001>

HOLT, T., BOSSLER, A., & SEIGFRIED-SPELLAR, K. (2022). *Cybercrime and Digital Forensics: An Introduction* (3rd ed.). Routledge. <https://doi.org/10.4324/9780429343223>

JACOMINO. D. Você é um profissional ético? *Você S.A.*, São Paulo, v.3, n.25, p.28-37,jul. 2000.

KAUFMAN, Dora; SANTAELLA, Lucia. O papel dos algoritmos de inteligência artificial nas redes sociais. *Revista FAMECOS*, [S. l.], v. 27, n. 1, p. e34074, 2020. DOI: <https://doi.org/10.15448/1980-3729.2020.1.34074>

MARQUES, L. G. Psicoterapia on-line: regulamentação e reflexo nas plataformas de atendimento. *Psicologia em Pesquisa*, v. 16, n. 3, p. 1-25, 2022. DOI: <https://doi.org/10.34019/1982-1247.2022.v16.32168>

MITTELSTADT, B. Principles alone cannot guarantee ethical AI. *Nat Mach Intell* 1, 501–507 (2019). <https://doi.org/10.1038/s42256-019-0114-4>

MÔCHO, J. O crescimento do comércio eletrônico no pós-pandemia e os desafios da legislação vigente. *Revista Eletrônica da OAB-RJ*, [S. l.], 2025.



MORLEY, J., ELHALAL, A., GARCIA, F. et al. Ethics as a Service: A Pragmatic Operationalisation of AI Ethics. *Minds & Machines* 31, 239–256 (2021). <https://doi.org/10.1007/s11023-021-09563-w>

NONAKA, I.; TAKEUCHI, H. *The Wise Company: How Companies Create Continuous Innovation*. Oxford: Oxford University Press, 2019.

NUNES, D. H.; LEHFELD, L. S. Cidadania digital: direitos, deveres, lides cibernéticas e responsabilidade civil no ordenamento jurídico brasileiro. *Revista de Estudos Jurídicos da UNESP, Franca*, v. 22, n. 35, 2019. DOI: <https://doi.org/10.22171/rej.v22i35.2542>

PRADO, A. P. P. Emoções Conectadas: Desvendando o impacto da inteligência emocional na liderança e gestão de pessoas na era digital. *REVISTA ACADÊMICA DA LUSOFONIA*, [S. l.], v. 2, n. 7, p. 1–11, 2025. DOI: <https://doi.org/10.69807/2966-0785.2025.115>

SANTOS, L.R; MARTINS, L.B; TYBUSCH, F.B.A. Os Crimes Cibernéticos E O Direito A Segurança Jurídica: Uma Análise Da Legislação Vigente No Cenário Brasileiro Contemporâneo. 4º Congresso Internacional de Direito e Contemporaneidade, 8 a 10 de novembro de 2017, Santa Maria/RS.

SANTOS, A. C. Variações conceituais entre a ética e a moral. *Filosofia Unisinos*, v. 22, n. 2, p. e22207, 2021. DOI: <https://doi.org/10.4013/fsu.2021.222.07>

SCHMITZ, A. H. (2025). O dano moral ao nascituro no contexto digital. *Revista Contemporânea*, 5(7), e8581. <https://doi.org/10.56083/RCV5N7-046>

SILVA BARBOSA, A. et al. Relações humanas e privacidade na internet: implicações bioéticas. *Revista de bioética y derecho*, n. 30, p. 109-124, 2014.

SIQUEIRA, D. P.; NUNES, D. H. Conflitos digitais: cidadania e responsabilidade civil no âmbito das lides cibernéticas. *Revista Jurídica da FA7*, v. 15, n. 2, p. 127-138, 2018.

TAMANDARÉ, A. F.; SEIDEL, G. S.; LEONARDELI, P. B. O impacto da tecnologia na leitura no ensino superior: desafios e possibilidades para a formação de leitores críticos no curso de pedagogia. *Revista Multidisciplinar do Nordeste Mineiro*, v. 10, n. 1, p. 1-33, 2025. DOI: <https://doi.org/10.61164/rmm.v10i1.4003>

TSAMADOS, A., AGGARWAL, N., COWLS, J. et al. The ethics of algorithms: key problems and solutions. *AI & Soc* 37, 215–230 (2022). <https://doi.org/10.1007/s00146-021-01154-8>

VERMELHO, Sônia Cristina; VELHO, Ana Paula Machado; BERTONCELLO, Valdecir. Sobre o conceito de redes sociais e seus pesquisadores. *Educação e Pesquisa*, v. 41, n. 4, p. 863-881, 2015. DOI: <https://doi.org/10.1590/s1517-97022015041612>

