REVISTA TÓPICOS
ISSN 2965-6672 | Qualis A2

DIREITOS HUMANOS NA ERA DIGITAL: DESAFIOS DA PROTEÇÃO DA DIGNIDADE HUMANA FRENTE À VIGILÂNCIA ALGORÍTMICA E AO USO DE DADOS PESSOAIS

HUMAN RIGHTS IN THE DIGITAL AGE: CHALLENGES IN PROTECTING HUMAN DIGNITY AGAINST ALGORITHMIC SURVEILLANCE AND THE USE OF PERSONAL DATA

Ciências Humanas, Ciências Sociais Aplicadas • 14/06/2026

REGISTRO DOI: 10.70773/revistatopicos/781478200

Rudney Ferreira Bonfi[1]

Thiago Daniel Ribeiro Tavares[2]

José Antonio da Silva[3]

Doriane Braga Nunes Bilac[4]

Victor Hugo da Silva Xisto[5]

Maria Eduarda Seemann[6]

Ana Caroline da Silva Taumaturgo[7]

Igor Bandeira de Matos[8]

RESUMO

O avanço das tecnologias digitais tem provocado transformações profundas nas relações sociais, econômicas, políticas e jurídicas, criando novas possibilidades de comunicação, inovação, participação democrática e desenvolvimento econômico. Ao mesmo tempo, a expansão da coleta massiva de dados pessoais, o uso de sistemas algorítmicos, a vigilância digital, a inteligência artificial, a biometria, a publicidade comportamental e as plataformas digitais têm produzido desafios complexos para a proteção dos direitos humanos. Este artigo analisa criticamente os impactos da vigilância algorítmica e do uso intensivo de dados pessoais sobre a dignidade humana, a privacidade, a autonomia, a igualdade, a liberdade de expressão e a autodeterminação informativa. A pesquisa adota abordagem qualitativa, de natureza bibliográfica e documental, com análise normativa de marcos jurídicos nacionais e internacionais, especialmente a Constituição Federal de 1988, a Lei Geral de Proteção de Dados Pessoais, o Regulamento Geral de Proteção de Dados da União Europeia, a Recomendação da UNESCO sobre Ética da Inteligência Artificial e o Regulamento Europeu de Inteligência Artificial. Argumenta-se que os marcos tradicionais de proteção de direitos, embora essenciais, mostram-se insuficientes diante das novas formas de controle digital baseadas em perfilização, predição, classificação automatizada e exploração econômica da atenção e do comportamento. Os resultados indicam que a proteção efetiva da dignidade humana na era digital exige transparência algorítmica, responsabilização das plataformas, governança de dados, auditoria independente, proteção contra discriminação automatizada, fortalecimento das autoridades reguladoras e garantia de participação democrática na regulação das tecnologias. Conclui-se que a inovação tecnológica deve ser subordinada aos direitos fundamentais, e não o contrário, sendo indispensável construir uma

ordem digital centrada na pessoa humana.

Palavras-chave: direitos humanos; privacidade digital; vigilância algorítmica; proteção de dados; dignidade humana; inteligência artificial.

ABSTRACT

The advancement of digital technologies has profoundly transformed social, economic, political, and legal relations, creating new possibilities for communication, innovation, democratic participation, and economic development. At the same time, the expansion of massive personal data collection, the use of algorithmic systems, digital surveillance, artificial intelligence, biometrics, behavioral advertising, and digital platforms has produced complex challenges for the protection of human rights. This article critically analyzes the impacts of algorithmic surveillance and the intensive use of personal data on human dignity, privacy, autonomy, equality, freedom of expression, and informational self-determination. The research adopts a qualitative, bibliographic, and documentary approach, with normative analysis of national and international legal frameworks, especially the Brazilian Federal Constitution of 1988, the Brazilian General Personal Data Protection Law, the European Union General Data Protection Regulation, the UNESCO Recommendation on the Ethics of Artificial Intelligence, and the European Artificial Intelligence Act. It argues that traditional rights protection frameworks, although essential, are insufficient in the face of new forms of digital control based on profiling, prediction, automated classification, and economic exploitation of attention and behavior. The results indicate that the effective protection of human dignity in the digital age requires algorithmic transparency, platform accountability, data governance, independent auditing, protection against automated discrimination, strengthening of regulatory

authorities, and democratic participation in technology regulation. The article concludes that technological innovation must be subordinated to fundamental rights, not the opposite, and that it is essential to build a human-centered digital order.
Keywords: human rights; digital privacy; algorithmic surveillance; data protection; human dignity; artificial intelligence.

1. INTRODUÇÃO

As tecnologias digitais tornaram-se parte estruturante da vida contemporânea. A comunicação, o consumo, o trabalho, a educação, a saúde, a segurança pública, a política, o lazer, os serviços bancários e as relações institucionais passaram a ser mediados por plataformas, aplicativos, bancos de dados, sistemas de inteligência artificial e mecanismos automatizados de decisão. Esse processo produziu benefícios importantes: ampliou o acesso à informação, acelerou serviços, facilitou transações, criou novas formas de participação social e permitiu inovação em diferentes setores. Contudo, também inaugurou um ambiente de riscos profundos para os direitos humanos.

Na sociedade digital, a pessoa humana é cada vez mais transformada em dado. Suas buscas, deslocamentos, compras, interações, preferências, opiniões, redes de contato, localização, biometria, padrões de consumo, hábitos de leitura, tempo de permanência em telas e reações emocionais podem ser coletados, armazenados, cruzados, analisados e utilizados para fins econômicos, políticos, securitários ou administrativos. O sujeito deixa de ser observado apenas por instituições específicas e passa a ser monitorado continuamente por infraestruturas digitais distribuídas.

Esse cenário produziu o que diversos autores chamam de capitalismo de vigilância, sociedade da vigilância, governamentalidade algorítmica ou dataficação da vida social. Shoshana Zuboff afirma que o capitalismo de vigilância se fundamenta na extração de excedentes comportamentais, isto é, na coleta e análise de dados sobre comportamentos humanos para prever e influenciar ações futuras. David Lyon, por sua vez, compreende a vigilância como processo de coleta e análise de informações pessoais para influenciar, administrar, proteger ou controlar populações. Cathy O'Neil alerta para os riscos de modelos matemáticos opacos que podem reforçar desigualdades sociais quando usados em decisões sobre crédito, emprego, educação, policiamento e acesso a oportunidades.

A vigilância algorítmica não se limita à observação. Ela envolve classificação, ranqueamento, predição e intervenção. Sistemas automatizados podem decidir quais conteúdos serão exibidos, quais pessoas receberão ofertas de crédito, quais currículos serão selecionados, quais cidadãos serão considerados suspeitos, quais consumidores pagarão preços diferentes, quais trabalhadores serão monitorados e quais grupos serão considerados de maior risco. Assim, os algoritmos passam a participar de decisões que afetam diretamente direitos, oportunidades e liberdades.

A dignidade humana, fundamento central dos direitos humanos, passa a ser tensionada por essas práticas. Se a dignidade pressupõe que cada pessoa deve ser tratada como sujeito de valor próprio, e não como objeto de manipulação, a exploração invisível de dados pessoais coloca em risco essa premissa. A pessoa pode ser reduzida a perfil, escore, probabilidade ou categoria estatística. Sua autonomia pode ser limitada por sistemas que induzem escolhas,

modulam comportamentos e filtram informações. Sua igualdade pode ser violada por algoritmos que reproduzem vieses sociais. Sua privacidade pode ser esvaziada por práticas de coleta permanente e consentimentos pouco transparentes.

A proteção de dados pessoais tornou-se, por isso, tema essencial dos direitos humanos contemporâneos. No Brasil, a Lei nº 13.709/2018, Lei Geral de Proteção de Dados Pessoais, disciplina o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou jurídica, com o objetivo de proteger direitos fundamentais de liberdade e privacidade e o livre desenvolvimento da personalidade da pessoa natural. (planalto.gov.br) Essa formulação é relevante porque conecta diretamente proteção de dados, liberdade, privacidade e personalidade.

No plano internacional, o Regulamento Geral de Proteção de Dados da União Europeia consolidou princípios como licitude, finalidade, minimização, exatidão, limitação da conservação, integridade, confidencialidade e responsabilização. O modelo europeu influenciou legislações em diferentes países e fortaleceu a compreensão de que dados pessoais não são simples ativos econômicos, mas extensões da personalidade e da vida privada. No campo da inteligência artificial, a União Europeia aprovou o Regulamento 2024/1689, conhecido como AI Act, estabelecendo regras harmonizadas para sistemas de IA e inaugurando o primeiro marco jurídico abrangente sobre inteligência artificial no mundo. (eur-lex.europa.eu) A Comissão Europeia apresenta o AI Act como a primeira estrutura legal abrangente sobre IA em nível mundial, voltada a promover uma inteligência artificial confiável. (digital-strategy.ec.europa.eu)

A UNESCO também estabeleceu referência internacional ao aprovar, em 2021, a Recomendação sobre a Ética da Inteligência Artificial, considerada o primeiro instrumento global de definição de padrões éticos para IA, aplicável aos 194 Estados-membros da organização. A UNESCO afirma que a proteção dos direitos humanos e da dignidade humana constitui a pedra angular da Recomendação, com base em princípios como transparência, justiça e supervisão humana. (unesco.org)

Apesar desses avanços, permanecem desafios significativos. A velocidade da inovação tecnológica supera frequentemente o ritmo de atualização dos marcos jurídicos. Plataformas digitais operam em escala transnacional, enquanto muitas regulações seguem limitadas por fronteiras nacionais. Algoritmos são frequentemente protegidos por segredo comercial, dificultando auditoria e transparência. O consentimento do usuário, em muitos casos, é formal, extenso e pouco compreensível. Além disso, a concentração econômica das grandes plataformas dificulta a responsabilização efetiva.

Diante disso, este artigo parte do seguinte problema de pesquisa: **quais são os principais desafios para a proteção da dignidade humana e dos direitos humanos frente à vigilância algorítmica e ao uso massivo de dados pessoais na era digital?**

O objetivo geral é analisar criticamente o impacto da vigilância algorítmica e do uso de dados pessoais sobre a dignidade humana e os direitos fundamentais. Como objetivos específicos, busca-se: a) discutir a relação entre dignidade humana, privacidade e proteção de dados; b) compreender a vigilância algorítmica como forma contemporânea de controle social; c) analisar os limites dos marcos regulatórios tradicionais diante das tecnologias digitais; d) examinar

princípios como transparência algorítmica, responsabilização e supervisão humana; e) propor caminhos para conciliar inovação tecnológica e proteção de direitos.

Defende-se como tese central que a proteção dos direitos humanos na era digital exige superar uma visão individualista e meramente consentimental da privacidade, avançando para modelos de governança pública, democrática e coletiva dos dados e algoritmos, com centralidade na dignidade humana.

2. METODOLOGIA

A pesquisa adota abordagem qualitativa, de natureza bibliográfica, documental e normativa. Essa escolha justifica-se porque o tema envolve análise crítica de conceitos jurídicos, filosóficos, tecnológicos e políticos, além da interpretação de marcos normativos nacionais e internacionais. Não se pretende realizar mensuração estatística de fenômenos digitais, mas compreender os impactos da vigilância algorítmica e do uso de dados pessoais sobre direitos fundamentais.

A pergunta norteadora da investigação foi: **de que maneira a vigilância algorítmica e o uso massivo de dados pessoais desafiam a proteção da dignidade humana e dos direitos humanos na era digital?**

A pesquisa bibliográfica fundamenta-se em autores reconhecidos nos campos dos direitos humanos, proteção de dados, sociedade da vigilância, filosofia da tecnologia e regulação digital. Entre os referenciais principais, destacam-se Stefano Rodotà, Danilo Doneda, Laura Schertel Mendes, Ingo Wolfgang Sarlet, Shoshana Zuboff, David Lyon, Cathy O'Neil, Frank Pasquale, Luciano Floridi, Byung-Chul Han, Julie Cohen, Mireille Hildebrandt e Hannah Arendt. Esses

autores contribuem para compreender privacidade, autodeterminação informativa, dignidade, vigilância, poder algorítmico, economia dos dados e riscos de discriminação automatizada.

A pesquisa documental e normativa considera marcos jurídicos e documentos institucionais, como:

a. Constituição da República Federativa do Brasil de 1988;

b. Lei Geral de Proteção de Dados Pessoais, Lei nº 13.709/2018;

c. Regulamento Geral de Proteção de Dados da União Europeia;

d. Recomendação da UNESCO sobre a Ética da Inteligência Artificial;

e. Regulamento Europeu de Inteligência Artificial, Regulamento 2024/1689;

f. documentos da Organização das Nações Unidas sobre privacidade, tecnologia e direitos humanos;

g. diretrizes internacionais sobre ética, transparência e responsabilização algorítmica.

Os critérios de inclusão das fontes foram: pertinência direta com direitos humanos, privacidade, proteção de dados, vigilância digital, inteligência artificial, algoritmos e regulação de plataformas; reconhecimento acadêmico ou institucional; atualidade normativa; e relevância para análise crítica da dignidade humana na era digital.

Foram excluídos materiais opinativos sem base acadêmica, textos comerciais de empresas de tecnologia, publicações sem autoria identificável e documentos que tratassem inovação tecnológica de forma exclusivamente econômica, sem relação com direitos fundamentais.

A análise foi organizada em oito categorias: a) dignidade humana e direitos fundamentais; b) privacidade e proteção de dados; c) vigilância algorítmica; d) autonomia e manipulação comportamental; e) discriminação algorítmica; f) transparência e explicabilidade; g) responsabilização das plataformas; h) governança democrática da tecnologia.

Por se tratar de estudo bibliográfico e documental, não houve coleta direta de dados pessoais ou participação de sujeitos humanos. Assim, não se aplica submissão a comitê de ética. Ainda assim, o estudo assume compromisso ético com a defesa da dignidade humana, da liberdade, da igualdade e da proteção contra novas formas de dominação digital.

3. DIGNIDADE HUMANA E DIREITOS HUMANOS NA SOCIEDADE DIGITAL

A dignidade humana constitui um dos fundamentos mais importantes do pensamento jurídico contemporâneo e ocupa posição central na proteção dos direitos humanos e dos direitos fundamentais. No constitucionalismo brasileiro, a dignidade da pessoa humana está expressamente prevista como um dos fundamentos da República Federativa do Brasil, conforme o artigo 1º, inciso III, da Constituição Federal de 1988. Essa previsão não possui apenas valor simbólico. Ela estabelece uma orientação normativa

para todo o ordenamento jurídico, impondo ao Estado, à sociedade e também aos agentes privados o dever de reconhecer cada ser humano como sujeito de valor próprio, portador de liberdade, autonomia, igualdade, privacidade, integridade e direitos invioláveis.

A dignidade humana impede que a pessoa seja tratada como objeto, instrumento ou meio para finalidades externas à sua própria condição humana. Em outras palavras, nenhum indivíduo pode ser reduzido a mercadoria, estatística, perfil, dado, risco ou simples recurso econômico. Essa afirmação, que já era fundamental nas relações sociais tradicionais, torna-se ainda mais relevante na sociedade digital, em que os indivíduos passam a ser constantemente monitorados, classificados, mensurados e convertidos em informações economicamente exploráveis. A dignidade, nesse novo contexto, precisa ser pensada também diante das formas digitais de instrumentalização da pessoa.

Ingo Wolfgang Sarlet compreende a dignidade da pessoa humana como uma qualidade intrínseca e distintiva reconhecida a cada ser humano, que o torna merecedor de respeito e consideração por parte do Estado e da comunidade. Essa compreensão envolve a proteção contra tratamentos degradantes, desumanizadores, discriminatórios ou instrumentalizadores. Também implica assegurar condições mínimas para que cada pessoa possa desenvolver sua personalidade, exercer sua autonomia e participar da vida social em igualdade de condições. Na era digital, a proteção contra tratamentos degradantes não se limita mais a impedir agressões físicas, censura direta ou violações materiais evidentes. Ela também deve alcançar formas mais sutis, invisíveis e automatizadas de violação da liberdade humana.

A sociedade digital amplia a capacidade de coleta, armazenamento e análise de informações pessoais em uma escala inédita. Dados sobre localização, consumo, preferências políticas, histórico de navegação, relações sociais, padrões de deslocamento, buscas na internet, interações em redes sociais, registros biométricos e comportamento em plataformas são continuamente capturados e processados. Esses dados podem ser utilizados para personalizar serviços, melhorar políticas públicas e facilitar atividades econômicas. Contudo, também podem ser empregados para vigilância, manipulação, discriminação, controle social e exploração comercial da intimidade.

Nesse cenário, a pessoa humana passa a correr o risco de ser reduzida a um conjunto de informações fragmentadas. Em vez de ser reconhecida em sua complexidade, história, subjetividade e autonomia, ela pode ser convertida em perfil de consumo, pontuação de risco, tendência comportamental, categoria estatística ou alvo de publicidade personalizada. Essa redução é incompatível com a dignidade humana quando impede que o indivíduo compreenda, controle ou conteste os usos de seus dados. A pessoa não pode ser transformada em objeto de predição e manipulação sem transparência, consentimento válido e mecanismos efetivos de proteção.

A vigilância algorítmica representa uma das expressões mais complexas desse problema. Diferentemente da vigilância tradicional, que dependia de observação direta, a vigilância digital opera de modo contínuo, automatizado e muitas vezes invisível. Ela não apenas registra comportamentos passados, mas tenta prever comportamentos futuros. Sistemas algorítmicos analisam grandes volumes de dados para identificar padrões, inferir preferências,

antecipar decisões e influenciar condutas. Com isso, a liberdade individual pode ser afetada mesmo sem coerção explícita. O indivíduo continua formalmente livre, mas suas escolhas passam a ser condicionadas por sistemas que organizam o que ele vê, consome, acredita, deseja ou teme.

Essa forma de controle é especialmente preocupante porque muitas vezes atua sem que a pessoa perceba. Sistemas de recomendação definem quais notícias, vídeos, produtos, pessoas ou discursos serão apresentados com maior destaque. Plataformas digitais organizam a visibilidade social e modulam a circulação de informações. Anúncios personalizados exploram fragilidades emocionais, hábitos de consumo e preferências políticas. Ferramentas automatizadas podem decidir quem terá acesso a crédito, emprego, seguro, benefício, vaga educacional ou oportunidade comercial. Quando esses processos são opacos, a dignidade humana é enfraquecida, pois a pessoa perde a capacidade de compreender as forças que influenciam sua vida.

A dignidade também se relaciona diretamente com a autonomia. Ser digno significa poder participar da construção da própria trajetória, tomar decisões relevantes, formar convicções e desenvolver a personalidade sem manipulação indevida. Na sociedade digital, a autonomia é ameaçada quando plataformas utilizam dados pessoais para induzir comportamentos, prolongar tempo de permanência, estimular consumo compulsivo, direcionar discursos políticos ou explorar vulnerabilidades psicológicas. A manipulação algorítmica não retira formalmente a liberdade, mas pode reduzir a capacidade real de escolha consciente.

Outro risco importante é a discriminação algorítmica. Sistemas automatizados podem reproduzir desigualdades históricas presentes nos dados utilizados para seu desenvolvimento. Um algoritmo de crédito pode penalizar moradores de determinadas regiões. Um sistema de seleção de currículos pode reproduzir padrões discriminatórios de gênero, raça ou classe social. Ferramentas de policiamento preditivo podem aumentar a vigilância sobre comunidades pobres e racializadas. Plataformas de educação podem classificar estudantes com base em dados incompletos, limitando oportunidades futuras. Quando decisões automatizadas produzem desigualdade sob aparência de neutralidade técnica, há grave ameaça à dignidade e aos direitos humanos.

A igualdade, nesse sentido, não pode ser compreendida apenas como ausência de discriminação explícita. Na era digital, a discriminação pode ocorrer por critérios indiretos, inferências estatísticas e correlações aparentemente neutras. O algoritmo pode não utilizar diretamente raça, gênero, renda ou deficiência, mas empregar variáveis que funcionam como substitutos dessas características. Por isso, a proteção da dignidade exige auditoria, transparência, avaliação de impacto e responsabilização. Não basta confiar na suposta objetividade da tecnologia. Sistemas digitais são produzidos por pessoas, instituições e interesses econômicos; portanto, carregam escolhas, valores e riscos.

Hannah Arendt, embora tenha escrito em contexto anterior à sociedade digital, oferece contribuição relevante ao discutir o espaço público, a liberdade e a ação humana. Para Arendt, a política depende da possibilidade de aparecer diante dos outros, falar, agir e participar da construção do mundo comum. Na sociedade digital,

esse espaço público passa a ser mediado por plataformas privadas que organizam a visibilidade dos discursos, definem regras de circulação de conteúdos e influenciam a formação da opinião pública. A mediação algorítmica afeta, portanto, a experiência democrática. Se determinados discursos são amplificados e outros invisibilizados por critérios opacos, a liberdade pública torna-se condicionada por estruturas privadas de poder informacional.

Essa questão é central para os direitos humanos porque a democracia depende de informação plural, debate público e participação livre. Plataformas digitais não são apenas ambientes neutros de comunicação; elas possuem modelos de negócio, critérios de recomendação, políticas de moderação e interesses econômicos. Quando a lógica de engajamento privilegia conteúdos polarizadores, sensacionalistas ou emocionalmente manipuladores, a esfera pública pode ser distorcida. A dignidade humana, nesse caso, é afetada não apenas no plano individual, mas também no plano coletivo, pois a formação livre da vontade democrática é comprometida.

A dataficação da vida social exige, portanto, reinterpretar a dignidade humana. A proteção da pessoa não pode limitar-se à defesa contra agressões físicas, censura direta ou invasões tradicionais de privacidade. É necessário proteger o indivíduo contra formas invisíveis de controle, exploração informacional, manipulação comportamental e discriminação automatizada. A pessoa deve ter direito de saber como seus dados são coletados, para quais finalidades são utilizados, por quanto tempo serão armazenados, com quem serão compartilhados e quais consequências podem produzir em sua vida.

Stefano Rodotà defende que a proteção de dados deve ser compreendida como componente essencial da cidadania contemporânea. Para o autor, a privacidade não é apenas o direito de ser deixado só, conforme a concepção clássica. Ela envolve o poder de controlar a circulação das informações pessoais e proteger a liberdade existencial dos indivíduos. Essa formulação é especialmente importante porque desloca a privacidade de uma dimensão meramente individual para uma dimensão política. Proteger dados é proteger liberdade, igualdade e democracia.

Danilo Doneda, no Brasil, contribuiu de forma decisiva para consolidar a ideia de proteção de dados como direito fundamental ligado à personalidade, à liberdade e à autodeterminação informativa. A autodeterminação informativa significa que o titular dos dados deve ter capacidade de conhecer e influenciar o tratamento de suas informações pessoais. Esse direito é indispensável em uma sociedade na qual decisões relevantes são tomadas com base em dados. Sem controle sobre os fluxos informacionais, a pessoa perde parte de sua autonomia e fica vulnerável a usos abusivos de suas informações.

A Lei Geral de Proteção de Dados Pessoais representa avanço importante nesse sentido, pois estabelece princípios como finalidade, adequação, necessidade, transparência, segurança, prevenção, não discriminação e responsabilização. Esses princípios procuram limitar o poder de quem coleta e utiliza dados pessoais. O princípio da finalidade impede usos genéricos e indefinidos. O princípio da necessidade exige que sejam tratados apenas os dados indispensáveis. O princípio da transparência obriga clareza sobre o tratamento. O princípio da não discriminação busca impedir usos

abusivos ou discriminatórios. O princípio da responsabilização impõe dever de prestação de contas aos agentes de tratamento.

Entretanto, a efetividade da proteção da dignidade humana na era digital não depende apenas da existência de leis. Depende também de fiscalização, educação digital, cultura de proteção de dados, atuação das autoridades reguladoras, responsabilidade das empresas e participação social. A complexidade técnica dos sistemas digitais pode dificultar o exercício dos direitos pelos cidadãos. Muitas pessoas não compreendem os termos de uso que aceitam, não sabem quais dados são coletados e não conseguem avaliar os riscos envolvidos. Por isso, a proteção da dignidade exige mecanismos coletivos e institucionais, e não apenas escolhas individuais.

A arquitetura informacional da sociedade passa a ser, portanto, uma dimensão fundamental dos direitos humanos. Sistemas digitais definem possibilidades de visibilidade, escolha, consumo, participação, vigilância e controle. Eles organizam o acesso à informação, influenciam relações sociais, mediam oportunidades econômicas e condicionam experiências políticas. Se essa arquitetura é construída apenas segundo interesses comerciais, sem transparência e sem controle democrático, a dignidade humana fica subordinada à lógica da exploração de dados.

A regulação dos dados e algoritmos torna-se, assim, questão central de direitos humanos. Regular não significa impedir inovação tecnológica, mas garantir que a inovação respeite a pessoa humana. A tecnologia deve servir ao desenvolvimento humano, e não transformar indivíduos em objetos de vigilância, manipulação ou lucro ilimitado. A defesa da dignidade na sociedade digital exige que

sistemas tecnológicos sejam avaliados segundo critérios de justiça, transparência, necessidade, proporcionalidade, segurança, explicabilidade e responsabilidade.

Também é necessário reconhecer que a proteção da dignidade digital possui dimensão coletiva. O uso de dados não afeta apenas indivíduos isolados, mas grupos inteiros. Dados de uma comunidade podem ser usados para classificá-la como área de risco. Dados de consumidores podem ser utilizados para manipular preços. Dados de eleitores podem orientar campanhas políticas personalizadas e invisíveis ao debate público. Dados de trabalhadores podem alimentar sistemas de monitoramento e avaliação automatizada. Assim, a proteção de dados é também proteção contra novas formas de desigualdade social.

A dignidade humana na sociedade digital exige, ainda, preservar espaços de privacidade, silêncio, anonimato relativo e liberdade de experimentação. A vida humana não pode ser integralmente monitorada, registrada e analisada. A possibilidade de errar, mudar de opinião, construir identidade e desenvolver pensamento próprio depende de espaços não submetidos à vigilância permanente. Quando tudo é registrado e potencialmente utilizado, a pessoa pode passar a se autocensurar, limitando sua liberdade existencial.

Dessa forma, os direitos humanos na era digital precisam ser compreendidos como instrumentos de contenção do poder informacional. No passado, a proteção de direitos foi desenvolvida para limitar o poder absoluto do Estado, impedir arbitrariedades e proteger liberdades individuais. Hoje, além do Estado, grandes plataformas e corporações digitais concentram poder sobre dados,

comunicação e comportamento. A proteção da dignidade exige enfrentar também essas formas privadas de poder.

Conclui-se que a dignidade humana continua sendo fundamento indispensável dos direitos humanos, mas sua proteção precisa ser atualizada diante da sociedade digital. A pessoa humana não pode ser reduzida a dado, perfil, mercadoria, escore ou objeto de manipulação algorítmica. A defesa da dignidade exige privacidade, proteção de dados, transparência, explicabilidade, não discriminação, autonomia e controle democrático das tecnologias. Na era da dataficação, proteger direitos humanos significa também regular as arquiteturas digitais que moldam a vida social. Somente assim será possível construir uma sociedade tecnológica verdadeiramente orientada pela liberdade, pela igualdade e pelo respeito à pessoa humana.

4. PRIVACIDADE, PROTEÇÃO DE DADOS E AUTODETERMINAÇÃO INFORMATIVA

A privacidade é um dos direitos mais impactados pela sociedade digital. Tradicionalmente, foi compreendida como esfera de intimidade, reserva e proteção contra ingerências indevidas. Contudo, na era dos dados, essa concepção tornou-se insuficiente. A privacidade não se refere apenas ao segredo, mas ao controle sobre informações pessoais e aos efeitos sociais de sua circulação.

A proteção de dados pessoais amplia essa perspectiva. Dados pessoais não são apenas informações isoladas; quando combinados, podem revelar aspectos íntimos, preferências políticas, religião, saúde, orientação sexual, localização, vínculos sociais, condições econômicas, hábitos de consumo e vulnerabilidades emocionais.

Mesmo dados aparentemente banais podem adquirir sensibilidade quando cruzados com outras bases.

A Lei Geral de Proteção de Dados Pessoais brasileira estabelece princípios como finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização. A lei tem como objetivo proteger direitos fundamentais de liberdade e privacidade e o livre desenvolvimento da personalidade. (planalto.gov.br) Esses princípios representam avanço relevante, pois impõem limites ao tratamento indiscriminado de dados.

A autodeterminação informativa é conceito fundamental nesse debate. Surgiu no contexto da jurisprudência alemã e refere-se ao direito de cada pessoa controlar, dentro de limites jurídicos, o uso de suas informações pessoais. Na sociedade digital, esse direito enfrenta dificuldades práticas. Usuários frequentemente aceitam termos de uso longos e incompreensíveis, sem real possibilidade de negociação. Plataformas coletam dados de forma contínua e indireta. Muitas decisões baseadas em dados ocorrem sem conhecimento do titular.

O consentimento, embora importante, não é suficiente como base exclusiva de proteção. A assimetria entre usuário e plataforma é enorme. O usuário depende de serviços digitais para trabalhar, estudar, comunicar-se, consumir e acessar direitos. Recusar termos pode significar exclusão social ou econômica. Além disso, mesmo quando consente, dificilmente compreende a complexidade dos fluxos de dados.

Por isso, a proteção de dados deve combinar direitos individuais, deveres institucionais e fiscalização pública. O titular deve ter direitos de acesso, correção, eliminação, portabilidade, informação e revisão de decisões automatizadas. Contudo, empresas e Estados também devem ter obrigações de minimização, segurança, governança, avaliação de impacto e prestação de contas. Autoridades reguladoras precisam ter independência e capacidade técnica para fiscalizar.

A privacidade digital é também direito coletivo. Quando plataformas coletam dados em massa, produzem efeitos que ultrapassam indivíduos isolados. Dados de um grupo podem ser usados para inferir características de outros grupos. Perfis coletivos podem orientar policiamento, propaganda política, seguros, crédito e políticas públicas. Assim, a proteção de dados é condição para igualdade, democracia e não discriminação.

5. VIGILÂNCIA ALGORÍTMICA E NOVAS FORMAS DE CONTROLE

A vigilância algorítmica consiste no monitoramento, coleta, processamento e análise automatizada de dados com a finalidade de classificar, prever, influenciar ou controlar comportamentos. Diferencia-se da vigilância tradicional por sua escala, velocidade, invisibilidade e capacidade preditiva. Não se limita a observar o que as pessoas fizeram; busca antecipar o que provavelmente farão.

David Lyon destaca que a vigilância contemporânea está incorporada a sistemas cotidianos, como cartões, câmeras, plataformas digitais, bancos de dados, aplicativos e redes sociais. Na era algorítmica, esses sistemas tornam-se ainda mais sofisticados,

pois não apenas armazenam informações, mas produzem inferências.

A vigilância algorítmica manifesta-se em diferentes contextos:

a. plataformas digitais que monitoram comportamento para publicidade direcionada;

b. aplicativos que coletam localização e padrões de uso;

c. sistemas de segurança pública baseados em reconhecimento facial;

d. escolas que monitoram desempenho e comportamento estudantil por plataformas;

e. empresas que monitoram produtividade de trabalhadores;

f. bancos que utilizam escores automatizados de crédito;

g. governos que cruzam bases de dados para identificar riscos, fraudes ou perfis;

h. sistemas de saúde que analisam dados sensíveis para triagem e previsão.

Essas práticas podem ter finalidades legítimas, como segurança, eficiência, prevenção de fraudes e melhoria de serviços. Contudo, também podem produzir violações. O problema não está apenas no uso de tecnologia, mas na ausência de limites, transparência, proporcionalidade, necessidade, controle democrático e possibilidade de contestação.

Byung-Chul Han argumenta que a sociedade digital transforma liberdade em mecanismo de controle, pois os indivíduos expõem voluntariamente informações que alimentam sistemas de vigilância. Essa leitura ajuda a compreender que a vigilância contemporânea não opera apenas pela coerção estatal, mas também pelo desejo de conexão, conveniência e reconhecimento social.

Shoshana Zuboff aprofunda esse diagnóstico ao afirmar que grandes plataformas extraem dados comportamentais para prever e modificar condutas. A vigilância, nesse modelo, torna-se base de acumulação econômica. A pessoa não é apenas usuária; é fonte de dados e objeto de predição.

A vigilância algorítmica desafia direitos humanos porque altera a relação entre indivíduo e poder. Quando a pessoa sabe ou suspeita que está sendo monitorada, pode modificar seu comportamento. Isso afeta liberdade de expressão, liberdade de associação e participação política. Além disso, quando sistemas automatizados classificam pessoas sem transparência, criam novas formas de exclusão.

6. AUTONOMIA, MANIPULAÇÃO COMPORTAMENTAL E PLATAFORMAS DIGITAIS

A autonomia é elemento central da dignidade humana. Ser autônomo significa poder formar preferências, tomar decisões, construir projetos de vida e agir sem manipulação indevida. Na era digital, essa autonomia é ameaçada por mecanismos algorítmicos que organizam informações, direcionam conteúdos e influenciam escolhas.

Plataformas digitais operam por sistemas de recomendação que definem o que será visto, ocultado ou priorizado. Esses sistemas são projetados para maximizar engajamento, tempo de permanência e interação. O problema é que conteúdos mais polarizadores, emocionais ou sensacionalistas podem gerar mais engajamento, mesmo quando prejudicam a qualidade do debate público.

A publicidade comportamental também afeta a autonomia. Anúncios são direcionados com base em perfis detalhados, vulnerabilidades, interesses e comportamentos anteriores. Em campanhas políticas, essa lógica pode ser usada para microdirecionamento de mensagens, explorando medos ou crenças específicas de grupos. A pessoa deixa de participar de uma esfera pública comum e passa a receber mensagens personalizadas, muitas vezes invisíveis aos demais.

Julie Cohen argumenta que a privacidade é condição para a liberdade intelectual e para a formação da subjetividade. Sem espaços de experimentação, anonimato relativo e controle sobre exposição, a autonomia fica comprometida. A vigilância contínua tende a moldar comportamentos e reduzir possibilidades de resistência.

O uso de dados pessoais também pode produzir manipulação econômica. Plataformas podem ajustar preços, ofertas e oportunidades com base em perfis. Sistemas de crédito podem negar acesso sem explicação clara. Empregadores podem utilizar análise automatizada para selecionar candidatos, reproduzindo vieses. Assim, a autonomia individual é limitada por decisões invisíveis.

A proteção da autonomia exige transparência sobre sistemas de recomendação, limites à publicidade comportamental, proteção contra padrões manipulativos, direito de contestar decisões automatizadas e educação digital crítica. Não basta proteger o dado isolado; é necessário proteger a capacidade humana de escolher livremente.

7. DISCRIMINAÇÃO ALGORÍTMICA E IGUALDADE

A promessa dos algoritmos muitas vezes é apresentada como neutralidade. Como modelos matemáticos operam por dados e regras computacionais, haveria menos subjetividade humana. Contudo, essa visão é equivocada. Algoritmos são construídos por pessoas, treinados com dados históricos, orientados por objetivos específicos e aplicados em contextos sociais marcados por desigualdades.

Cathy O'Neil chama atenção para modelos opacos e prejudiciais que podem ampliar desigualdades. Frank Pasquale, em The Black Box Society, discute como sistemas algorítmicos protegidos por segredo dificultam fiscalização, contestação e responsabilização. Esses autores demonstram que a opacidade algorítmica é problema democrático.

A discriminação algorítmica pode ocorrer de diversas formas. Dados históricos podem refletir desigualdades raciais, de gênero, territoriais ou econômicas. Um sistema de recrutamento treinado com dados de contratações passadas pode reproduzir preferências discriminatórias. Um sistema de policiamento preditivo pode direcionar maior vigilância a áreas pobres e racializadas, reforçando ciclos de criminalização. Um sistema de crédito pode penalizar

pessoas de determinados territórios. Um sistema educacional pode classificar estudantes de forma injusta com base em dados incompletos.

A igualdade, como direito humano, exige não apenas tratamento formalmente igual, mas proteção contra discriminações estruturais. Na era algorítmica, isso significa auditar dados, modelos e resultados. Não basta afirmar que o algoritmo não usa raça, gênero ou deficiência se outras variáveis funcionam como substitutos indiretos. CEP, padrão de consumo, escola frequentada, rede de contatos e histórico familiar podem reproduzir desigualdades.

A UNESCO estabelece que a proteção dos direitos humanos e da dignidade humana deve orientar a ética da IA, com princípios como justiça, não discriminação, transparência e supervisão humana. (unesco.org) O AI Act europeu adota abordagem baseada em risco, impondo obrigações mais severas para sistemas de alto risco, inclusive aqueles que afetam direitos, segurança e oportunidades. (digital-strategy.ec.europa.eu)

No Brasil, a LGPD inclui o princípio da não discriminação, vedando tratamento de dados para fins discriminatórios ilícitos ou abusivos. (planalto.gov.br) Esse princípio é essencial para enfrentar decisões automatizadas injustas. Contudo, sua efetividade depende de fiscalização, capacidade técnica, transparência e acesso a mecanismos de contestação.

8. TRANSPARÊNCIA ALGORÍTMICA, EXPLICABILIDADE E RESPONSABILIZAÇÃO

A transparência algorítmica é um dos principais desafios da era digital. Sistemas automatizados afetam decisões relevantes, mas

frequentemente operam de forma opaca. Usuários não sabem quais dados são coletados, como são processados, quais critérios são utilizados, quais inferências são produzidas e como decisões são tomadas.

A explicabilidade refere-se à capacidade de oferecer razões compreensíveis sobre o funcionamento ou resultado de um sistema algorítmico. Em decisões que afetam direitos, a explicabilidade é condição de devido processo, contestação e responsabilização. Se uma pessoa tem crédito negado, benefício bloqueado, perfil classificado como risco ou conteúdo removido, precisa compreender os fundamentos da decisão.

A transparência não exige necessariamente divulgação integral de código-fonte em todos os casos. Pode envolver documentação, auditorias, relatórios de impacto, explicações sobre variáveis relevantes, testes de viés, avaliação de riscos, governança interna e prestação de contas a autoridades. O ponto central é impedir que o segredo tecnológico torne impossível a proteção de direitos.

A responsabilização das plataformas é igualmente essencial. Durante muito tempo, grandes empresas digitais foram tratadas como intermediárias neutras. Contudo, plataformas organizam visibilidade, moderam conteúdos, definem regras de circulação, monetizam dados e influenciam comportamentos. Portanto, devem responder por impactos de seus sistemas.

A responsabilização deve incluir:

a. dever de transparência sobre coleta e uso de dados;

b. avaliação de impacto sobre direitos fundamentais;

c. auditoria independente de sistemas de alto risco;

d. mecanismos de contestação acessíveis;

e. reparação por danos;

f. dever de segurança da informação;

g. proteção de crianças e grupos vulneráveis;

h. combate a discriminação automatizada;

i. governança de inteligência artificial;

j. fiscalização por autoridades públicas.

A UNESCO destaca a importância de supervisão humana de sistemas de IA e de princípios como transparência e justiça. (unesco.org) O AI Act europeu também representa avanço ao diferenciar sistemas por nível de risco e impor obrigações específicas a desenvolvedores e implantadores de IA. (eur-lex.europa.eu)

No Brasil, a Autoridade Nacional de Proteção de Dados tem papel central na aplicação da LGPD, mas a complexidade dos sistemas algorítmicos exige fortalecimento institucional, recursos técnicos e cooperação com outros órgãos reguladores. A regulação digital não pode depender apenas de ações individuais de titulares; precisa de fiscalização estruturada.

9. LIMITES DOS MARCOS REGULATÓRIOS TRADICIONAIS

Os marcos tradicionais de proteção de direitos foram construídos em um contexto no qual as violações eram mais facilmente identificáveis: censura direta, invasão de domicílio, interceptação de comunicação, discriminação explícita, abuso estatal visível. Na era digital, muitas violações são invisíveis, distribuídas, automatizadas e transnacionais.

A primeira limitação é a dificuldade de identificação da violação. O indivíduo pode não saber que foi classificado, ranqueado, excluído ou manipulado por um sistema. Sem conhecimento, não há contestação.

A segunda limitação é a escala. Uma decisão algorítmica pode afetar milhões de pessoas rapidamente. A reparação individual, embora necessária, pode ser insuficiente.

A terceira limitação é a transnacionalidade. Dados circulam por diferentes países, servidores e empresas. Isso dificulta jurisdição, fiscalização e responsabilização.

A quarta limitação é a assimetria técnica. Usuários, juízes, legisladores e até reguladores podem ter dificuldade de compreender sistemas complexos. Empresas detêm expertise e infraestrutura muito superiores.

A quinta limitação é a dependência social das plataformas. Serviços digitais tornaram-se quase indispensáveis. Isso limita a liberdade real de escolha dos usuários.

A sexta limitação é a insuficiência do consentimento. Termos de uso extensos e opacos não garantem autonomia informativa.

A sétima limitação é a concentração econômica. Poucas empresas controlam grandes volumes de dados, infraestrutura digital e ecossistemas de comunicação.

Esses limites demonstram que a proteção de direitos humanos na era digital exige atualização regulatória. Não basta aplicar categorias antigas sem adaptação. É necessário desenvolver instrumentos como avaliação de impacto algorítmico, auditoria obrigatória, deveres fiduciários de dados, transparência pública, regulação de plataformas, proteção coletiva de dados e direitos contra decisões automatizadas injustas.

10. RESULTADOS DA ANÁLISE

A análise bibliográfica e normativa permite identificar seis resultados principais.

O primeiro resultado é que a dignidade humana tornou-se vulnerável a formas invisíveis de instrumentalização digital. A pessoa pode ser tratada como fonte de dados, perfil comportamental ou objeto de predição, reduzindo sua autonomia e singularidade.

O segundo resultado é que a privacidade precisa ser compreendida de forma ampliada. Não se trata apenas de esconder informações íntimas, mas de controlar fluxos informacionais que afetam liberdade, igualdade e personalidade.

O terceiro resultado é que a vigilância algorítmica amplia o poder de Estados e empresas sobre indivíduos e populações. Esse poder não opera apenas pela repressão, mas pela predição, modulação e personalização de estímulos.

O quarto resultado é que a discriminação algorítmica representa risco concreto aos direitos humanos. Sistemas automatizados podem reproduzir desigualdades históricas sob aparência de neutralidade técnica.

O quinto resultado é que os marcos regulatórios estão avançando, mas ainda enfrentam dificuldades de aplicação. A LGPD, o GDPR, a Recomendação da UNESCO e o AI Act representam respostas importantes, mas dependem de fiscalização, recursos técnicos e cooperação internacional.

O sexto resultado é que a proteção efetiva exige governança democrática da tecnologia. Transparência, responsabilização, auditoria, participação social e supervisão humana são indispensáveis.

11. DISCUSSÃO

A principal discussão deste artigo é que a era digital exige uma reconfiguração da proteção dos direitos humanos. As tecnologias digitais não são apenas ferramentas neutras; elas estruturam relações de poder, definem visibilidades, classificam sujeitos e moldam comportamentos. Por isso, a proteção da dignidade humana precisa alcançar também as arquiteturas digitais.

A vigilância algorítmica desafia a noção clássica de liberdade. Uma pessoa pode não ser formalmente coagida, mas pode ter suas escolhas influenciadas por sistemas que exploram seus dados e vulnerabilidades. Pode não ser censurada diretamente, mas pode receber informações filtradas por algoritmos que moldam sua visão de mundo. Pode não ser discriminada explicitamente, mas pode ser excluída por modelos opacos.

A privacidade, nesse contexto, torna-se condição de autonomia. Sem privacidade, não há espaço para formação livre da personalidade. Sem proteção de dados, a pessoa perde controle sobre dimensões essenciais de sua vida. Sem transparência algorítmica, não há possibilidade real de contestação.

Outro ponto central é que a regulação não deve ser vista como obstáculo à inovação. Pelo contrário, direitos fundamentais são condição para inovação legítima. Tecnologias que violam dignidade, discriminam ou manipulam não devem ser celebradas como progresso. A inovação precisa estar subordinada a valores democráticos.

A discussão também revela que a proteção de dados deve ser coletiva. A lógica individual do consentimento é limitada. É necessário proteger grupos, comunidades e populações contra usos abusivos de dados. Isso inclui crianças, trabalhadores, consumidores, minorias raciais, pessoas pobres, pessoas com deficiência e outros grupos vulnerabilizados.

A transparência algorítmica também deve ser proporcional ao impacto. Sistemas usados para recomendações simples não exigem o mesmo nível de controle que sistemas utilizados em segurança pública, crédito, saúde, educação ou emprego. Quanto maior o risco aos direitos, maior deve ser o dever de explicação, auditoria e responsabilização.

Por fim, a governança digital precisa ser democrática. Decisões sobre tecnologias que afetam a sociedade não podem ficar restritas a empresas privadas e especialistas técnicos. É necessário envolver

juristas, educadores, movimentos sociais, usuários, comunidades afetadas, reguladores e pesquisadores.

12. PROPOSTAS PARA PROTEÇÃO DA DIGNIDADE HUMANA NA ERA DIGITAL

A partir da análise, podem ser propostas diretrizes para proteção dos direitos humanos frente à vigilância algorítmica.

Primeiro, fortalecer a proteção de dados pessoais como direito fundamental, garantindo aplicação efetiva da LGPD e atuação robusta da autoridade reguladora.

Segundo, exigir avaliações de impacto sobre direitos fundamentais em sistemas algorítmicos de alto risco.

Terceiro, implementar auditorias independentes de algoritmos utilizados em decisões relevantes.

Quarto, garantir transparência e explicabilidade em decisões automatizadas que afetem direitos.

Quinto, assegurar direito à contestação humana de decisões automatizadas.

Sexto, proibir ou restringir usos abusivos de reconhecimento facial e vigilância biométrica em massa.

Sétimo, responsabilizar plataformas digitais por danos decorrentes de sistemas de recomendação, coleta abusiva de dados ou discriminação algorítmica.

Oitavo, proteger crianças e adolescentes contra exploração de dados, publicidade comportamental abusiva e manipulação digital.

Nono, promover educação digital crítica para cidadãos compreenderem riscos e direitos.

Décimo, estimular cooperação internacional para enfrentar fluxos transnacionais de dados e poder das grandes plataformas.

13. CONCLUSÃO

A era digital trouxe possibilidades inéditas de comunicação, inovação e desenvolvimento, mas também produziu novas formas de risco aos direitos humanos. A vigilância algorítmica e o uso massivo de dados pessoais desafiam diretamente a dignidade humana, a privacidade, a autonomia, a igualdade e a liberdade. A pessoa humana corre o risco de ser reduzida a perfil, dado, escore ou previsão comportamental.

O estudo demonstrou que a proteção dos direitos humanos na era digital exige atualização dos instrumentos jurídicos e políticos. A privacidade não pode ser compreendida apenas como segredo individual, mas como condição de autonomia, liberdade e democracia. A proteção de dados não é tema técnico ou burocrático; é dimensão essencial da cidadania contemporânea.

A LGPD representa avanço relevante no Brasil ao proteger direitos fundamentais de liberdade, privacidade e livre desenvolvimento da personalidade. (planalto.gov.br) No plano internacional, a Recomendação da UNESCO sobre Ética da IA e o AI Act europeu indicam caminhos importantes para transparência, supervisão humana, justiça e responsabilização. (unesco.org) (eur-lex.europa.eu)

Entretanto, normas formais não bastam. É necessário garantir fiscalização, capacidade técnica, auditorias, participação social e responsabilização efetiva das plataformas e dos agentes que utilizam dados e algoritmos. A dignidade humana precisa ser protegida não apenas contra abusos visíveis, mas também contra formas invisíveis de manipulação, classificação e discriminação.

Conclui-se que a inovação tecnológica deve ser orientada por direitos humanos. A pergunta central não deve ser apenas o que a tecnologia pode fazer, mas o que ela deve fazer em uma sociedade democrática. O progresso digital só será legítimo se fortalecer liberdade, igualdade, autonomia, justiça e dignidade. Caso contrário, a tecnologia deixará de ser instrumento de emancipação e se converterá em mecanismo sofisticado de controle.

REFERÊNCIAS BIBLIOGRÁFICAS

ARENDT, Hannah. **A condição humana.** Rio de Janeiro: Forense Universitária, 2010.

BRASIL. **Constituição da República Federativa do Brasil de 1988.** Brasília, DF: Presidência da República, 1988.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais. Brasília, DF: Presidência da República, 2018.

COHEN, Julie E. **Between truth and power: the legal constructions of informational capitalism.** Oxford: Oxford University Press, 2019.

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

EUROPEAN UNION. **Regulation (EU) 2016/679: General Data Protection Regulation.** Brussels: European Union, 2016.

EUROPEAN UNION. **Regulation (EU) 2024/1689: Artificial Intelligence Act.** Brussels: European Union, 2024.

FLORIDI, Luciano. **The ethics of information.** Oxford: Oxford University Press, 2013.

HAN, Byung-Chul. **Psicopolítica: o neoliberalismo e as novas técnicas de poder.** Belo Horizonte: Âyiné, 2018.

HILDEBRANDT, Mireille. **Smart technologies and the end(s) of law: novel entanglements of law and technology.** Cheltenham: Edward Elgar, 2015.

LYON, David. **Surveillance studies: an overview.** Cambridge: Polity Press, 2007.

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

O'NEIL, Cathy. **Weapons of math destruction: how big data increases inequality and threatens democracy.** New York: Crown, 2016.

PASQUALE, Frank. **The black box society: the secret algorithms that control money and information.** Cambridge: Harvard University Press, 2015.

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

SARLET, Ingo Wolfgang. **Dignidade da pessoa humana e direitos fundamentais na Constituição Federal de 1988.** Porto Alegre: Livraria do Advogado, 2015.

UNESCO. **Recommendation on the Ethics of Artificial Intelligence.** Paris: UNESCO, 2021.

UNITED NATIONS. **The right to privacy in the digital age.** Geneva: United Nations, 2021.

ZUBOFF, Shoshana. **The age of surveillance capitalism: the fight for a human future at the new frontier of power.** New York: PublicAffairs, 2019.

---

[1] Mestre em Educação e Graduando em Direito pela Faculdade de Itaituba. E-mail: acesse o artigo original para visualizar o e-mail

[2] Doutor pela Universidade Federal de São Carlos (UFSCar), Mestre pela Universidade de Ribeirão Preto (UNAERP) e Bacharel em Direito pela Universidade de Araraquara (UNIARA). Atua no Instituto Municipal de Bebedouro-SP (IMESB). E-mail: acesse o artigo original para visualizar o e-mail

[3] Doutorando em Ciências Jurídicas pela São Luiz University (SLU), Licenciado em Filosofia e Pedagogia. Atua como Mediador Judicial no Tribunal de Justiça do Estado do Rio de Janeiro (TJRJ).

[4] Doutora em Sociologia pela Universidade de Brasília (UnB). Atua na Universidade Federal do Tocantins (UFT). E-mail: acesse o artigo original para visualizar o e-mail

[5] Mestre em Estudos Jurídicos com ênfase em Direito Internacional pela MUST University (Florida - USA). E-mail: acesse o artigo original para visualizar o e-mail

[6] Graduanda em Direito pela Universidade do Vale do Itajaí (UNIVALI). E-mail: acesse o artigo original para visualizar o e-mail

[7] Graduanda em Direito pelo Centro Universitário do Norte (UNINORTE). E-mail: acesse o artigo original para visualizar o e-mail

[8] Pós-graduado em Direito Penal e Processo Penal pela Universidade do Vale do Itajaí (Univali). E-mail: acesse o artigo original para visualizar o e-mail