REVISTA DCS
FUNDADA EN 2000

DADOS COMO MOEDA, PRIVACIDADE COMO LIMITE: A NECESSIDADE DE NORMAS *EX ANTE* PERANTE O PODER INFORMACIONAL DA INTELIGÊNCIA ARTIFICIAL

DATA AS CURRENCY, PRIVACY AS A LIMIT: THE NEED FOR EX ANTE REGULATION IN THE FACE OF THE INFORMATIONAL POWER OF ARTIFICIAL INTELLIGENCE

LOS DATOS COMO MONEDA DE CAMBIO, LA PRIVACIDAD COMO LÍMITE: LA NECESIDAD DE NORMAS EX ANTE ANTE EL PODER INFORMACIONAL DE LA INTELIGENCIA ARTIFICIAL

Lorena de Almeida Nunes[1], Lucas Almeida da Rocha Lago[2], Caio Pereira de Oliveira[3], Kaio Oliveira de Souza[4], Maria Alice Tanan Mangabeira[5], Ingride Cruz da Silva[6]

DOI: 10.54899/dcs.v23i87.4298
Recibido: 20/01/2026 | Aceptado: 23/01/2026 | Publicación en línea: 18/02/2026.

RESUMO

A Quarta Revolução Industrial inaugura um novo paradigma socioeconômico caracterizado pela centralidade dos dados como principal ativo estratégico da atividade produtiva, especialmente os dados pessoais, realocando os fatores tradicionais de capital, trabalho e organização industrial. Nesse contexto, a Inteligência Artificial (IA) desponta como uma nova camada informacional, dotada da capacidade de processar volumes massivos de dados, identificar padrões complexos e realizar inferências preditivas, impactando de forma profunda as estruturas sociais, econômicas, políticas e jurídicas contemporâneas. A crescente adoção de sistemas automatizados de tomada de decisão, alimentados por grandes bases de dados pessoais, suscita relevantes preocupações quanto à proteção dos direitos fundamentais, em especial a privacidade, a autodeterminação informativa, a igualdade, a não discriminação e o devido processo legal. Nessa senda floresce a questão norteadora: em que medida as decisões automatizadas, alimentadas por grandes volumes de dados pessoais, ameaçam os direitos fundamentais na era da inteligência artificial? Para tanto, adota-se uma abordagem qualitativa, de natureza exploratória, com base em pesquisa bibliográfica e documental, analisando a doutrina especializada, marcos normativos e diretrizes

[1] Mestranda em Direito pela Universidade Federal da Bahia (UFBA), Universidade do Estado da Bahia (UNEB), Salvador, Bahia, Brasil. E-mail: lorenanunes@ufba.br Orcid: https://orcid.org/0000-0002-7288-7734
[2] Mestrando em Direito pela Universidade Federal da Bahia (UFBA), Universidade do Estado da Bahia (UNEB), Salvador, Bahia, Brasil. E-mail: advlago@advlago.com Orcid: https://orcid.org/0009-0006-0881-270
[3] Mestrando em Psicologia do Desenvolvimento pela Universidade Federal da Bahia (UFBA), Universidade do Estado da Bahia (UNEB), Salvador, Bahia, Brasil. E-mail: psi.caiocpo@gmail.com
Orcid: https://orcid.org/0000-0001-6937-5511
[4] Pós-Graduando em Processo Civil pela Pontifícia Universidade Católica do Rio Grande do Sul (PUCRS), União Metropolitana para o Desenvolvimento da Educação e Cultura (UNIME), Salvador, Bahia, Brasil.
E-mail: kaiosouza.dominio@gmail.com
[5] Especialista em Ciências Criminais pela Universidade Católica de Salvador (UCSAL), Universidade do Estado da Bahia (UNEB), Salvador, Bahia, Brasil. E-mail: atmangabeira@gmail.com
[6] Mestrando em Ciências Sociais pela Universidade Federal do Recôncavo da Bahia (UFRB), Universidade do Estado da Bahia (UNEB), Salvador, Bahia, Brasil. E-mail: ingridecruzadv@hotmail.com

regulatórias. Conclui-se que a IA atua como catalisadora de um novo regime de poder, racionalidade e justiça, exigindo do ordenamento jurídico brasileiro uma atuação ativa, orientada pelos princípios da transparência, da proporcionalidade, da explicabilidade e da responsabilização algorítmica, a fim de assegurar a centralidade da pessoa humana no ambiente digital.

Palavras-chave: Inteligência Artificial. Dados Pessoais. Informação. Privacidade.

ABSTRACT

The Fourth Industrial Revolution ushers in a new socioeconomic paradigm characterized by the centrality of data as the main strategic asset of productive activity, especially personal data, reallocating the traditional factors of capital, labor, and industrial organization. In this context, Artificial Intelligence (AI) emerges as a new layer of information, equipped with the ability to process massive volumes of data, identify complex patterns, and make predictive inferences, profoundly impacting contemporary social, economic, political, and legal structures. The growing adoption of automated decision-making systems, fed by large personal databases, raises significant concerns about the protection of fundamental rights, in particular privacy, informational self-determination, equality, non-discrimination, and due process of law. This raises the guiding question: to what extent do automated decisions, fed by large volumes of personal data, threaten fundamental rights in the age of artificial intelligence? To this end, a qualitative, exploratory approach is adopted, based on bibliographic and documentary research, analyzing specialized doctrine, normative frameworks, and regulatory guidelines. It is concluded that AI acts as a catalyst for a new regime of power, rationality, and justice, requiring the Brazilian legal system to take active measures, guided by the principles of transparency, proportionality, explainability, and algorithmic accountability, in order to ensure the centrality of the human person in the digital environment.

Keywords: Artificial Intelligence. Personal Data. Information. Privacy.

RESUMEN

La Cuarta Revolución Industrial inaugura un nuevo paradigma socioeconómico caracterizado por la centralidad de los datos como principal activo estratégico de la actividad productiva, especialmente los datos personales, reubicando los factores tradicionales de capital, trabajo y organización industrial. En este contexto, la Inteligencia Artificial (IA) surge como una nueva capa informativa, dotada de la capacidad de procesar volúmenes masivos de datos, identificar patrones complejos y realizar inferencias predictivas, lo que tiene un profundo impacto en las estructuras sociales, económicas, políticas y jurídicas contemporáneas. La creciente adopción de sistemas automatizados de toma de decisiones, alimentados por grandes bases de datos personales, suscita importantes preocupaciones en cuanto a la protección de los derechos fundamentales, en especial la privacidad, la autodeterminación informativa, la igualdad, la no discriminación y el debido proceso legal. En este sentido, surge la pregunta fundamental: ¿en qué medida las decisiones automatizadas, alimentadas por grandes volúmenes de datos personales, amenazan los derechos fundamentales en la era de la inteligencia artificial? Para ello, se adopta un enfoque cualitativo, de naturaleza exploratoria, basado en la investigación bibliográfica y documental, analizando la doctrina especializada, los marcos normativos y las directrices reguladoras. Se concluye que la IA actúa como catalizadora de un nuevo régimen de poder, racionalidad y justicia, exigiendo al ordenamiento jurídico brasileño una actuación activa,

orientada por los principios de transparencia, proporcionalidad, explicabilidad y responsabilidad algorítmica, con el fin de garantizar la centralidad de la persona humana en el entorno digital.

Palabras clave: Inteligencia Artificial. Datos Personales. Información. Privacidad.

INTRODUÇÃO

Na era da hiperconectividade, com os avanços das tecnologias de comunicação e informação, os indivíduos produzem, de forma contínua e muitas vezes inconsciente, rastros digitais que revelam suas preferências, hábitos e comportamentos. Essas interações contribuem para a constituição de um vasto repositório de dados pessoais, que inauguram um novo paradigma que transmuta as estruturas econômicas, sociais, e jurídicas (Zuboff, 2019).

Os dados, nesse contexto, assumem uma posição estratégica no epicentro da atividade produtiva, deslocando os tradicionais fatores de produção. Logo, os dados pessoais, ativos econômicos de altíssimo valor, tornam-se o principal insumo das dinâmicas decisórias e operacionais tanto no setor privado quanto nas esferas públicas (Varoufakis, 2025); impondo a necessidade de contínua adaptação dos marcos normativos às rápidas e disruptivas inovações tecnológicas, traço distintivo da Quarta Revolução Industrial (Schwab, 2019).

O presente diagnóstico encontra eco tanto nas análises sobre o que se convencionou chamar de capitalismo de vigilância, que concentra poderes preditivos e normativos em plataformas em hiperescala (Zuboff, 2018, p. 23), quanto nas formulações que descrevem uma mutação mais ampla do capital, apontando para um novo arranjo que alguns autores denominam tecnofeudalismo (Varoufakis, 2025, p. 41-45).

A arquitetura algorítmica e as infraestruturas em nuvem não são meros instrumentos de eficiência, tornam-se agenciamentos sociotécnicos capazes de transformar observações dispersas em conhecimento acionável, de modular comportamentos e de exercer condutas discretas de governança por meio de experimentação e personalização (Varoufakis, 2025).

Nesse galgar, a vigilância distribuída, a qual é alimentada por sensores, plataformas, sistemas de inteligência artificial (IA), dispositivos móveis e ecossistemas de internet das coisas (IOT), reconfigura fronteiras clássicas entre público e privado, entre consumidores e cidadãos,

produzindo efeitos que impactam tanto as relações de mercado quanto às garantias fundamentais (Firmino, 2018, p. 79-84).

A convergência entre os diagnósticos socioeconômicos e argumentos jurídico-normativos conduz, portanto, a duas constatações normativas: (i) que a proteção da privacidade e da autodeterminação informativa não se sustenta apenas por remédios *ex post*, sendo necessária uma arquitetura preventiva capaz de incidir sobre o desenho das tecnologias e sobre os modelos de governança de dados (Cardoso, 2018, p. 101-103);

E (ii) que essa arquitetura deve ser construída mediante critérios que integrem eficácia, transparência e responsabilização algorítmica sem sacrificar, de modo desproporcional, valores constitucionais essenciais (Alexy, 2011, p. 21-23).

Nesse ínterim, o surto pandêmico atuou, assim, como um verdadeiro catalisador para a digitalização em larga escala. A pesquisa realizada pelo Instituto Capgemini (2020) revelou que o Brasil se destacou nas interações cotidianas com sistemas de IA, o estudo indicou que o país ocupa a segunda posição no ranking mundial em termos de frequência de uso dessas tecnologias, superando, inclusive, a média global.

De acordo com a Pesquisa de Inovação Semestral (Pintec), divulgada pelo Instituto Brasileiro de Geografia e Estatística (IBGE) no primeiro semestre de 2025, observa-se um crescimento expressivo no uso de tecnologias de IA pela indústria brasileira. O levantamento revelou que, em apenas dois anos, o número de empresas industriais que utilizam IA saltou 163%, passando de 1.619 companhias em 2022 para 4.261 em 2024. Em termos proporcionais, 41,9% das empresas industriais pesquisadas já faziam uso da tecnologia em 2024, frente a 16,9% no período anterior (IBGE, 2025).

A pesquisa, realizada com uma amostra de 1.731 empresas industriais dentre um universo de 10.167 companhias com 100 ou mais empregados, também apontou que o uso de IA é mais recorrente nas organizações de maior porte. Entre as empresas com 500 ou mais trabalhadores, o percentual de adoção alcança 57,5%, enquanto nas faixas de 250 a 499 empregados e de 100 a 249 empregados os índices são de 42,5% e 36,1%, respectivamente (IBGE, 2025).

Esses dados evidenciam não apenas a expansão da incorporação da IA no setor produtivo nacional, mas também a tendência de intensificação tecnológica correlata ao porte empresarial, indicando um avanço progressivo da digitalização industrial no Brasil.

No contexto latino-americano, o Brasil desponta como líder tanto na adoção quanto no desenvolvimento de soluções baseadas em IA, com especial ênfase em aplicações voltadas à

internet e ao setor empresarial, como chatbots, assistentes virtuais e outras ferramentas digitais inovadoras (Capgemini, 2020).

Diante desse panorama, o presente artigo tem como objeto de estudo a relação entre a sociedade da informação, a inteligência artificial e os riscos à privacidade decorrentes do uso massivo de dados pessoais. A pergunta que orienta esta investigação é: em que medida as decisões automatizadas, alimentadas por grandes volumes de dados pessoais, ameaçam os direitos fundamentais na era da inteligência artificial, e como o ordenamento jurídico brasileiro pode responder a esses desafios?

Como objetivo geral, busca-se analisar os impactos da inteligência artificial sobre a privacidade e a proteção de dados na sociedade da informação. Especificamente, pretende-se: (i) contextualizar o surgimento da sociedade da informação e os seus desdobramentos tecnológicos; (ii) examinar a função dos dados pessoais na lógica algorítmica; (iii) examinar violações a direitos fundamentais por desvios funcionais da IA .

Nesse cenário, a tutela dos direitos da personalidade assume papel central no ordenamento jurídico, abarcando dimensões como a privacidade, a integridade física e psíquica, a imagem, a reputação e a autodeterminação informativa, elementos essenciais para a preservação da dignidade da pessoa humana frente ao avanço das tecnologias digitais.

REFERENCIAL TEÓRICO

Evolução dos Paradigmas: da Sociedade da Informação à Economia do Conhecimento

O conceito de Sociedade da Informação recebeu notoriedade nas décadas de 1970 e 1980, substituindo o conceito de "sociedade pós-industrial", e inserindo o novo paradigma técnico-econômico, que nasce do desenvolvimento de tecnologias computacionais e de telecomunicações que revolucionaram a forma como a informação é produzida, armazenada, distribuída e consumida; assumindo a posição que outrora foi ocupada pela terra ou pelo capital industrial (Castells, 2020).

O termo foi cunhado por sociólogos e economistas como Daniel Bell (1973), que introduziu o entendimento em seu livro "O advento da sociedade pós-industrial"; Pierre Lévy (1993), que identificou esse fenômeno como uma "revolução cognitiva" ao compreender a informação como vetor que altera modos de pensar, agir e interagir; e, Manuel Castells (1996),

que desenvolveu a teoria da “sociedade em rede”, na qual, os fluxos de informação globalizados substituem as formas tradicionais de organização social.

A sociedade da informação emerge, portanto, como um fenômeno em resposta às transformações estruturais das revoluções tecnológicas e pela globalização, esculpindo um novo paradigma civilizacional. A essência desse fenômeno está intimamente ligada ao termo “economia do conhecimento”, no qual, o conhecimento e a informação tornam-se os principais fatores de produção, substituindo em importância os recursos materiais tradicionais (Burch, 2006).

Nesse sentido, compreender a Sociedade da Informação significa reconhecer tanto suas promessas de democratização do conhecimento quanto os novos riscos que emergem da concentração do poder informacional em poucos atores (Zuboff, 2018, p. 27-30). Conforme destaca Castells (1996), vivencia-se uma nova economia estruturada em redes e baseada na geração, processamento e transmissão de informações por meio das tecnologias da informação e comunicação (TICs), rompendo com os modelos produtivos baseados exclusivamente no capital físico ou na força de trabalho manual.

A Organização para a Cooperação e Desenvolvimento Econômico (OCDE) também corrobora tal compreensão ao afirmar que, na economia do conhecimento, a produção, distribuição e uso do conhecimento e da informação tornam-se o fator chave para o crescimento econômico, a riqueza e o bem-estar (OCDE, 1996). Assim, a informação passa a ser tratada como um ativo estratégico, e sua gestão eficaz constitui requisito para a competitividade no mercado globalizado.

Assmann (2000) evidencia com precisão a transição provocada pelas novas tecnologias e seus impactos estruturais; essa transformação não se limita à ampliação da memória ou da velocidade de acesso à informação, mas alcança a própria forma de processar, organizar e interpretar dados. As tecnologias contemporâneas operam não apenas como instrumentos de armazenamento, mas como mecanismos de recombinação informacional, capazes de identificar padrões complexos e estabelecer conexões antes imperceptíveis ao intelecto humano.

Essa transição marca o advento de uma nova racionalidade econômica, centrada na informação, no conhecimento e na inovação tecnológica como elementos estratégicos. Castells (1996) assinala que tal fenômeno é consequência direta da reestruturação do capitalismo iniciada na década de 1980, a qual deu origem a uma economia em rede, flexível e globalizada, na qual os fluxos de informação assumem papel determinante para a geração de valor e poder.

O que se apresenta como inclusão digital e circulação livre de informações é, ao mesmo tempo, um modelo de vigilância difusa e dataficação sistêmica. Firmino (2018, p. 79) explica que o cotidiano, mediado por dispositivos digitais e sensores, converte-se em fonte permanente de dados. Esse movimento leva o que Zuboff (2018) denomina "capitalismo de vigilância", em que dados comportamentais são capturados para prever e influenciar condutas.

A crítica mais recente de Varoufakis (2025, p. 52-60) aprofunda essa análise ao sugerir que não se trata apenas de um capitalismo digitalizado, mas de um tecnofeudalismo, onde grandes plataformas operam como senhores feudais modernos. Assim, o ideal de sociedade conectada, convive com uma prática de exploração informacional, em que usuários tornam-se matéria-prima de um sistema econômico que captura seus dados para gerar valor.

Nesse processo de transformação estrutural, as TICs exercem papel central na reorganização dos modelos sociais, econômicos e institucionais contemporâneos. Tal processo foi impulsionado por avanços contínuos em hardware, software e infraestrutura de rede, os quais permitiram a consolidação de um ambiente altamente interconectado, dinâmico e globalizado, onde o acesso e a disseminação da informação ocorrem de forma instantânea e descentralizada (Varoufakis, 2025).

Lévy (1999) corrobora essa visão ao afirmar que o ciberespaço, formado pelas interações digitais mediadas pelas TICs, constitui um novo espaço antropológico, onde os saberes circulam de maneira inédita, transformando as formas de conhecimento, de cooperação e de exercício da cidadania. Nesse galgar, Schwab (2019), ao analisar a Quarta Revolução Industrial, ressalta que a convergência das tecnologias digitais, físicas e biológicas redesenham as fronteiras entre os mundos real e virtual, impactando radicalmente os sistemas de produção e as instituições sociais.

O cenário esboçado representa um desafio tanto tecnológico quanto ético, pois, enquanto ampliam-se as capacidades cognitivas, também devem-se considerar as implicações de tais capacidades na privacidade, segurança e na estrutura social. Do ponto de vista jurídico, esse cenário impõe desafios significativos, exigindo a reformulação de marcos normativos voltados à proteção de dados, à privacidade, ao acesso à informação e à autodeterminação informacional.

A Constituição Federal de 1988, em seu artigo 5º, incisos IX, XIV e XXXIII, reconhece o direito à informação como fundamental, o que, à luz da sociedade da informação, deve ser interpretado de forma dinâmica e adequada à nova realidade tecnológica.

Além disso, a promulgação da Lei nº 12.965/2014, Marco Civil da Internet, e da Lei nº 13.709/2018, Lei Geral de Proteção de Dados Pessoais (LGPD) evidencia o esforço normativo

brasileiro em adaptar-se à lógica da sociedade informacional, especialmente no que diz respeito à garantia dos direitos fundamentais no ambiente digital.

Outroassim, o estudo da Sociedade da Informação não pode se limitar à análise descritiva do fenômeno, mas deve buscar fundamentar critérios normativos que orientem sua regulação, garantindo que o avanço tecnológico se dê em consonância com os valores constitucionais.

Nessa conjuntura, a compreensão da informação perante IA exige um aprofundamento que transcende sua mera definição técnica. A IA não é apenas uma ferramenta de processamento de dados; ela representa uma nova camada informacional que remodela as estruturas sociais, econômicas e políticas (Bruno *et al.*, 2018; Varoufakis, 2025).

Para Floridi (2018), a IA pode ser vista como uma nova camada de informação, que precisa ser incorporada à nossa compreensão do mundo e da realidade. Esta camada de informação é a capacidade de processar grandes volumes de dados e identificar padrões e relações que seriam difíceis de serem identificados.

O *machine learning* (ML) ou aprendizagem de máquina, o sistema de IA extrai informações dos dados inseridos e faz seu aprendizado automático. O algoritmo analisa grandes volumes de dados, identifica padrões e produz previsões ou decisões com base nessas informações (Russell, Norvig, 2020). O sistema se adapta e aprende na medida em que as informações vão sendo por ele acumuladas (Bengio, 2014) sem que tenham sido programados para tal finalidade.

O *deep learning* (DL), ou aprendizagem profunda, é o modo em que a máquina aprende representações de dados em múltiplos níveis de abstração, assemelhando-se às redes neurais humanas. No livro "*Deep Learning*" (2016), Goodfellow, Bengio e Courville fornecem uma visão abrangente sobre o DL.

Os autores descreveram como as redes neurais profundas são capazes de extrair características e padrões complexos dos dados, utilizando várias camadas de processamento não-linear (Goodfellow *et al.*, 2016). É um método sofisticado de aprendizagem que incorpora sucessivas e infinitas camadas ocultas de redes neurais a partir de dados inseridos (Goodfellow *et al.*, 2016). Sua capacidade engloba a percepção e a assimilação de múltiplos e complexos comportamentos e padrões.

A explicação oferecida pelos citados autores quanto a operacionalidade e os mecanismos subjacentes, destaca a importância da informação e dos dados como recursos vitais para o desenvolvimento e eficácia desses sistemas (Goodfellow *et al.*, 2016). Este conceito se alinha

com a ideia de IA como um sistema que não apenas executa tarefas, mas também aprende e se adapta autonomamente. Já que, no contexto o qual está inserido a IA, os dados funcionam como o "alimento" para os algoritmos.

Essa maior disponibilidade de recursos tecnológicos, de acesso à informação e de dados pessoais, decorre do *big data*, o qual permite que os sistemas de IA se afastem do modelo de regras pré-fixadas e passem a fundamentar suas decisões e formar seus padrões decisionais no influxo de dados (Zuboff, 2018).

> Big data é uma expressão que remete a todo o influxo de dados que são coletados contra a nossa vontade e criam um perfil, de modo a expor nossa privacidade. Com efeito, ele é constituído pela captura de small data, das ações e discursos, mediados pelo computador, de indivíduos no desenrolar da vida prática. Nada é trivial ou efêmero em excesso para essa colheita: as "curtidas" do Facebook, as buscas no Google, e-mails, textos, fotos, músicas e vídeos, localizações, padrões de comunicação, redes, compras, movimentos, todos os cliques (ZUBOFF, pág 33, 2018).

Esses dados, nomeados de "*small data*", são acumulados em escala massiva e transformados em *Big Data*, que em suma, é o imenso volume de dados gerados continuamente por interações digitais diárias. Uma das críticas mais severas de Zuboff (2018) ao *Big Data* é a forma como os dados são frequentemente coletados sem consentimento claro e informado. Eles afetam a autonomia individual, e podem levar a uma sociedade onde as decisões e oportunidades estão cada vez mais determinadas por algoritmos.

Isso pode reforçar desigualdades existentes e criar novas formas de discriminação digital, onde os perfis baseados em dados influenciam tudo, desde ofertas de emprego até decisões de crédito (Requião e Costa, 2022).

Logo, a capacidade da IA de processar vastas quantidades de dados, identificar padrões complexos e a autoaprendizagem, coloca-a no cerne de uma transformação que redefine as relações de poder e as noções de autonomia e privacidade (Requião e Costa, 2022). Nesse modelo, as grandes corporações tecnológicas deixam de ser meras provedoras de serviços para se tornarem extratoras de uma nova matéria-prima: o comportamento humano, manifestado como dados (Varoufakis, 2025).

A IA é o motor desse sistema, pois é ela quem transforma o rastro digital deixado pelos usuários em matéria-prima de predição (Bruno *et al.*, 2018). Essa extração de dados não se limita a um consentimento livre e informado; ela se dá em um ambiente de doação compulsória de dados. Assim, a IA consolida um poder que não é mais fundado na posse de capital físico, mas

no controle dos dados e na capacidade de monetizar a vida cotidiana.

Varoufakis (2025), por sua vez, eleva essa análise a um novo patamar, argumentando que a IA e as plataformas digitais não apenas modificaram o capitalismo, mas o suplantaram por um "tecnofeudalismo". Diferentemente do capitalismo, que se baseava em lucros obtidos por meio de preços e mercados, a nova ordem extrai renda das nuvens. As grandes plataformas, ou "capitalistas-nuvem", não operam com base na competição por lucros, mas sim no controle de seus "feudos digitais", onde a troca de mercadorias é mediada por algoritmos (Varoufakis, 2025).

A IA é a peça-chave desse sistema, pois não apenas organizam e gerenciam as interações, mas também determinam as oportunidades e os limites de ação, transformando os usuários em vassalos (Varoufakis, 2025). A promessa de liberdade e eficiência das tecnologias digitais oculta uma nova forma de servidão, onde a autonomia da vontade é substituída pela submissão aos ditames algorítmicos.

Assim, a informação perante a Inteligência Artificial não se restringe a uma análise de dados, mas sim a uma disputa sobre quem controla e lucra com essa nova economia (Varoufakis, 2025). A IA, como um catalisador de um novo regime econômico e político, desafia as noções jurídicas tradicionais e exige uma reavaliação dos direitos fundamentais, da soberania e da dignidade humana na era da informação.

A discussão, portanto, se move da coleta de dados para uma análise crítica de como a IA está remodelando as fundações da nossa sociedade e qual o papel do direito em garantir que essa transformação não resulte em novas formas de servidão e controle.

A PRIVACIDADE E PROTEÇÃO DOS DADOS PESSOAIS NA ERA DA INTELIGÊNCIA ARTIFICIAL

A capacidade da IA era restrita aos dados armazenados localmente nos computadores, que operavam de forma isolada. Isso limitava significativamente o potencial dos sistemas, uma vez que dependiam exclusivamente das informações disponíveis na memória dessas máquinas (Haenlein, Kaplan, 2019). Contudo, os avanços tecnológicos permitiram a extração e análise de dados de maneira mais eficiente e precisa (Goodfellow, Bengio, Courville, 2016).

O fenômeno da conectividade global advindo da internet permitiu que os sistemas de IA acessassem dados instantaneamente. Nessa direção, a computação em nuvem possibilitou o armazenamento e processamento de enormes volumes de dados em grandes servidores,

eliminando as restrições de capacidade das memórias locais (Armbrust *et al*., 2010). Este desenvolvimento elevou a IA a assumir uma nova dimensão, pois possibilitou o acesso a informações *ad infinitum*.

A IA não apenas utiliza os dados pessoais, mas também os reconfigura, transformando a vida privada em um insumo econômico (Bruno *et al.*, 2018). A IA, por meio da análise de grandes volumes de dados (big data), é capaz de inferir padrões, prever ações futuras e, em última instância, influenciar decisões, o que impõe um novo desafio à autonomia individual e à proteção da privacidade.

A crise da privacidade emerge como uma consequência direta de uma nova ordem econômica e social, que monetiza as informações pessoais e transforma a vida cotidiana em uma fonte de valor (Bruno *et al.*, 2018). Nesse contexto, a privacidade colide com as lógicas de poder do novo regime tecnopolítico.

A informação pessoal, que antes era marginal, agora é o ativo central. Essa exploração não ocorre de forma passiva; ela se dá por meio de um complexo sistema de coleta, análise e monetização, onde a IA é a principal ferramenta para transformar comportamentos em produtos preditivos (Requião e Costa, 2022). Assim, a privacidade não é violada por um "erro" do sistema, mas sim como parte intrínseca de seu modelo de negócio (Requião e Costa, 2022). A privacidade é o preço a ser pago para se ter acesso a serviços que, na superfície, parecem ser "gratuitos".

Varoufakis (2025) preleciona como a privacidade é um dos principais tributos pagos pelos usuários. A coleta massiva de dados, a vigilância constante e a capacidade de direcionar e modular comportamentos transformam os usuários em “vassalos digitais”. Eles não são mais trabalhadores ou consumidores no sentido tradicional, que, ao usar as plataformas, doam sua atenção e seus dados, garantindo a acumulação de poder e riqueza dos "senhores-nuvem" (Varoufakis, 2025). A privacidade, nesse quadro, é a última fronteira de resistência à total mercantilização da experiência humana.

O direito à privacidade, tradicionalmente concebido como o direito a ser deixado em paz, assume uma nova e complexa dimensão na era da informação. Não se trata apenas da proteção do segredo ou da intimidade, mas da salvaguarda da autonomia individual em um contexto de vigilância tecnológica ubíqua. A privacidade se torna, nesse sentido, um contraponto essencial à lógica de extração de valor que caracteriza o “capitalismo de vigilância” (Bruno *et al.*, 2018).

Nesse regime, a privacidade não é apenas um direito a ser respeitado, mas um recurso a ser extraído. As plataformas digitais, operadas por inteligência artificial, coletam e monetizam os

dados pessoais, transformando a vida privada em um insumo econômico (Bruno *et al.*, 2018). O direito à privacidade, portanto, é diretamente confrontado por essa nova economia da vigilância, que opera com a premissa de que a vida humana é uma fonte inesgotável de dados comportamentais. Essa extração compulsória de dados ameaça a própria noção de "espaço privado", pois a fronteira entre o público e o privado é constantemente erodida pela arquitetura das plataformas e pela ausência de transparência sobre o uso das informações.

Para Varoufakis, essa ameaça à privacidade é um dos pilares do "tecnofeudalismo", onde a doação de dados pessoais se equipara ao pagamento de um tributo feudal (Varoufakis, 2025). O direito à privacidade, nessa perspectiva, é o direito a não ser submetido a essa nova forma de servidão digital. O controle sobre os dados pessoais é fundamental para que o indivíduo não se torne um mero "vassalo" dos "senhores-nuvem", que acumulam poder e riqueza por meio da vigilância e da manipulação algorítmica.

O direito à privacidade é um princípio fundamental reconhecido em diversas legislações, sendo uma peça chave para a dignidade, liberdade e desenvolvimento individual. Outrossim, a problemática que cerceia o direito à privacidade se iniciou nos Estados Unidos em 1890, quando os juristas Samuel D. Warren e Louis D. Brandeis publicaram o artigo "*The Right to Privacy*" na Harvard Law Review, no qual introduziram a ideia do direito ao esquecimento ("right to be let alone", em tradução: o direito de ser deixado em paz) (Silva, 2017).

Este conceito emergiu como uma resposta às crescentes invasões de privacidade causadas pelo avanço das tecnologias e pela imprensa sensacionalista. Identificando a necessidade de proteger a dignidade e a individualidade contra invasões injustificadas (Silva, 2017). Conceito revolucionário que ampliou a ideia de proteção legal para incluir não apenas danos físicos ou econômicos, mas também danos emocionais e psicológicos causados pela intrusão na vida privada de uma pessoa.

Nessa perspectiva, Ingo Wolfgang Sarlet (2015) define o direito à privacidade como um desdobramento do direito à dignidade, que permite ao indivíduo a possibilidade de controlar a divulgação de informações pessoais e de evitar ingerências indevidas em sua esfera privada. A privacidade pode ser entendida como o direito de estar livre de interferências ou intrusões indesejadas.

A Declaração Universal dos Direitos Humanos (art. 12) é um dos primeiros documentos a reconhecer a privacidade como um direito humano fundamental. O Pacto Internacional sobre os Direitos Civis e Políticos (art. 17), também proclama o direito de cada indivíduo de não ser

submetido a interferências arbitrárias ou ilegais em sua vida privada.

No contexto da legislação moderna, o direito à privacidade se estende a várias dimensões, incluindo a proteção de dados pessoais (Brasil, 2022). Afinal, diante dos avanços constantes das tecnologias, existe o desafio sem precedentes para a privacidade, o que tem levantado questões sérias sobre a eficácia das leis de privacidade existentes.

Para Alexy (2014), os direitos fundamentais não são apenas normas programáticas, mas princípios que, ao colidirem, devem ser ponderados. O direito deve ser capaz de institucionalizar a razão prática, ou seja, de fornecer uma base para decisões que não se limitem à mera legalidade, mas que reflitam um julgamento moralmente correto capaz de proteger o indivíduo.

Em suma, a relação entre a Sociedade da Informação e a privacidade é uma questão de poder, economia e justiça. A privacidade é um direito fundamental a ser defendido e readequado diante de novas formas de dominação.

O desafio de preservar a privacidade na Sociedade da Informação exige uma readequação jurídica que transcenda a simples compensação *ex post* (Cardoso, 2018). Nesse sentido, a arquitetura regulatória deve ser preventivamente construída, incidindo sobre o design das tecnologias e sobre os modelos de governança de dados (Cardoso, 2018).

O Regulamento da Inteligência Artificial (*AI Act*) da União Europeia (2024), ao buscar um regime jurídico uniforme e promover uma Inteligência Artificial centrada no ser humano e de confiança, atua diretamente nessa frente, reconhecendo a necessidade de proteger os direitos fundamentais, como a privacidade e a proteção de dados pessoais, consagrados na Carta (União Europeia, 2024).

É crucial notar que o IA não substitui, mas complementa, a legislação de proteção de dados já em vigor, como o Regulamento Geral de Proteção de Dados (Regulamento UE 2016/679) e as diretivas específicas para IA (2018). O direito fundamental à proteção de dados pessoais é explicitamente salvaguardado por esses instrumentos. As regras harmonizadas estabelecidas pelo *AI Act* para a colocação no mercado e utilização de sistemas de IA, portanto, visam reforçar a aplicação efetiva e permitir o exercício dos direitos dos titulares de dados (União Europeia, 2024).

Para garantir a coesão entre a inovação tecnológica e o respeito aos direitos, o *AI Act* incorpora o conceito de "proteção de dados desde a conceção e por norma" (*Privacy by Design and Default*), aplicável ao longo de todo o ciclo de vida do sistema de IA (União Europeia, 2024). As medidas implementadas pelos prestadores devem incluir a minimização dos dados e a

utilização de tecnologias que permitam o treinamento de sistemas sem a transmissão de dados brutos, sempre em conformidade com os requisitos de governação de dados estabelecidos no Regulamento (União Europeia, 2024).

A governança e a qualidade dos dados são requisitos mandatórios, especialmente para os sistemas de IA de alto risco, visando mitigar vieses e prevenir a discriminação. Os conjuntos de dados de treino, validação e teste devem ser pertinentes, suficientemente representativos e, na medida do possível, isentos de erros e completos. O regulamento europeu exige que os prestadores tenham uma atenção especial à atenuação de eventuais vieses nos conjuntos de dados que sejam suscetíveis de afetar negativamente os direitos fundamentais ou conduzir a discriminações proibidas pelo direito da União (União Europeia, 2024).

Nesse ínterim, dados podem ser descritos como representações simbólicas de fatos, eventos ou ocorrências que são coletados, armazenados e processados para diversos fins. Esses elementos podem assumir diferentes formas, como números, textos, imagens, sons, ou qualquer outra representação digital (Davenport, Prusak, 1998). Conforme Davenport e Prusak (1998), dados são transformados em conhecimento quando são organizados e processados de maneira a adquirir utilidade e relevância, ou seja, os dados são o substrato essencial do qual se extrai o conhecimento.

Yuval Noah Harari observa que a economia global contemporânea não se sustenta mais prioritariamente em recursos materiais. Em sua obra “Homo Deus: Uma Breve História do Amanhã” (2016), Harari argumenta que antes, as principais fontes de riqueza eram os recursos materiais, como minas de ouro, campos de trigo e poços de petróleo. Hoje, a principal fonte de riqueza é o conhecimento (Harari, 2016, p. 25).

Harari (2016) ao pontuar sobre a transição da economia global de recursos materiais para o conhecimento reflete uma mudança paradigmática na forma como a riqueza é gerada e sustentada. A transformação para uma economia baseada no conhecimento tem profundas implicações para o corpo social. De acordo com Thomas Davenport e Laurence Prusak em “*Working Knowledge: How Organizations Manage What They Know*” (1998), as organizações que conseguem captar, disseminar e utilizar o conhecimento de maneira eficaz têm uma vantagem competitiva significativa.

Este fenômeno pode ser observado na ascensão de indústrias baseadas em tecnologia, como a informática, biotecnologia e inteligência artificial. Peter Drucker, em “*Post-Capitalist Society*” (1993), antecipou essa mudança ao identificar o conhecimento como o recurso crucial

para a produtividade e a competitividade no século XXI. Assim, as empresas mais valiosas do mundo não são aquelas que possuem vastos recursos naturais, mas aquelas que dominam a inovação tecnológica e a gestão do conhecimento.

A inovação existe através da capacidade de extrair insights significativos dos dados. Essas técnicas permitem identificar padrões, prever tendências e tomar decisões informadas que podem transformar setores inteiros, desde a saúde até as finanças e a administração pública (Provost , Fawcett, 2013).

Perante evidências empíricas que mostram como a IA pode infringir direitos fundamentais, levantando uma necessidade urgente de reflexão jurídica sobre como promover o desenvolvimento dessas tecnologias e seus benefícios, enquanto se protege prioritariamente a segurança e privacidade dos direitos dos indivíduos que as utilizam ou são afetados por elas (Requião e Costa, 2022).

A displicência normativa diante da difusão exponencial cria uma conjuntura de insegurança jurídica significativa. Nessa direção, Nicholas Diakopoulos (2019), em "*Automating the News: How Algorithms Are Rewriting the Media*", pontua que a falta de normatização eficaz pode levar a violações de direitos fundamentais dos cidadãos, pois as operações das ferramentas de IA podem causar danos inadvertidos

Isto posto, a privacidade passou a ser cada vez mais associada à informação, com um foco particular nos dados pessoais. À medida que nossa sociedade se estrutura em torno da coleta e circulação de informações, surge um novo instrumento fundamental, ligado ao estabelecimento de novas dinâmicas ou relações de poder, que é a legitimidade do poder baseado na informação, tanto no contexto estatal quanto na indústria.

METODOLOGIA

A presente investigação ancora-se em uma abordagem qualitativa de natureza exploratória, utilizando o método hipotético-dedutivo para analisar o fenômeno do poder informacional. A base procedimental consiste em revisão bibliográfica exaustiva e análise documental, abrangendo o estado da arte na doutrina nacional e internacional, bem como o escrutínio crítico dos marcos legais vigentes e em tramitação.

A justificativa do estudo reside na assimetria de poder gerada pelo avanço disruptivo das Tecnologias de Informação e Comunicação (TICs). Embora tais inovações ofereçam ganhos de

eficiência, elas impõem ao Direito o ônus de mitigar riscos sistêmicos à dignidade humana na biosfera digital.

O cerne da problemática reside nas decisões automatizadas: operadas por matrizes estatísticas em ambientes de Big Data, tais processos exercem influência direta sobre a autonomia privada e a equidade social. No ecossistema da IA, a coleta e o tratamento de dados pessoais deixam de ser meras etapas técnicas para se tornarem vetores de poder, demandando uma arquitetura jurídica que priorize a autodeterminação informativa e a responsabilidade *ex ante*.

RESULTADOS E DISCUSSÕES

Violações a Direitos Fundamentais por Desvios Funcionais da IA: Casos Emblemáticos

Os desvios funcionais da inteligência artificial (IA), que resultam em violações de direitos fundamentais, não devem ser vistos como meras anomalias técnicas, mas como manifestações de uma estrutura de poder e controle em consolidação (Bruno *et al.*, 2018). Esses desvios são emblemáticos de um sistema que, por sua natureza, subordina a dignidade humana à lógica de acumulação de dados e de capital-nuvem.

Uma das violações mais evidentes decorre do viés algorítmico, que perpetua e amplifica discriminações existentes. Os desvios funcionais da IA ocorrem quando esses sistemas agem de forma imprevisível ou discriminatória, causando danos aos indivíduos ou grupos, ou quando realizam a coleta e processamento indevidos de dados pessoais, sem o consentimento informado dos indivíduos afetados (Requião e Costa, 2022).

Na China foi implementado um sistema de IA pelo governo com fins de medir a credibilidade social dos cidadãos (Requião e Costa, 2022). Este sistema realiza uma vigilância em massa de seus comportamentos socioeconômicos e políticos, utilizando dados coletados da internet, através do *big data*, para pontuar os mais de 1,3 bilhão de habitantes, julgando se são confiáveis ou não. A partir dessa análise, são atribuídas pontuações de crédito social, resultando em tratamentos diferenciados: indivíduos com pontuações altas recebem benefícios, enquanto aqueles com pontuações baixas enfrentam restrições de direitos (Times, 2022).

Todavia, meses após essa iniciativa, o próximo passo do Governo Chinês foi a identificação dos cidadãos apenas pela forma de andar. Ou seja, uma nova maneira de explorar a IA para a vigilância (El País, 2018). A experiência chinesa serve como um alerta para a

necessidade de estabelecer limites claros e mecanismos de proteção para o uso de tecnologias de vigilância. Frank Pasquale (2015) destaca que a vigilância constante pode ter um efeito de resfriamento na expressão livre, limitando a liberdade de pensamento e de associação.

Outro caso emblemático sobre invasão à vida privada de cidadãos através de ferramentas de IA, refere-se à empresa *Cambridge Analytica* (Hern, 2018). Esses dados foram usados para criar perfis psicológicos detalhados dos usuários, permitindo a segmentação de mensagens políticas para influenciar o comportamento eleitoral nas eleições presidenciais dos Estados Unidos em 2016 (Hern, 2018).

Utilizou para tanto sistemas de IA, através do *big bata*, para analisar em larga escala dados pessoais obtidos de forma não autorizada de milhares de usuários do Facebook. Cruzando informações e traçando padrões comportamentais e psicológicos, comprometendo a integridade do processo democrático ao manipular a opinião pública com base em informações pessoais obtidas de forma ilega (Hern, 2018).

Outro caso alarmante das complexidades envolvidas no uso de IA para a coleta e análise de dados pessoais em grande escala. Adveio da empresa *Clearview AI*, que desenvolveu um *software* que utilizava IA para analisar bilhões de imagens de rostos coletadas de várias fontes na internet, incluindo redes sociais, sem o consentimento dos indivíduos representados nessas imagens.

Ampliando horizontes, Catherine O'Neil (2016) argumenta que os algoritmos podem perpetuar e ampliar as desigualdades sociais. Um exemplo notório é o caso do sistema COMPAS (*Correctional Offender Management Profiling for Alternative Sanctions*), utilizado no sistema judiciário dos Estados Unidos para prever a probabilidade de reincidência criminal. Estudos demonstraram que o COMPAS tendia a superestimar o risco de reincidência para réus negros, o que configura discriminação racial e violação ao princípio da igualdade.

Nick Bostrom, filósofo reconhecido por suas contribuições no campo da IA e riscos existenciais, frequentemente discute as implicações sociais e éticas dos avanços em inteligência artificial. Segundo Bostrom (2014), à medida que os algoritmos assumem essas funções, eles também herdam as complexidades e responsabilidades sociais associadas, exigindo uma abordagem regulatória que reflita esses desafios. Ou seja, os algoritmos de IA ao se ocuparem de trabalho cognitivo com dimensões sociais, o algoritmo herda, da mesma forma, exigências sociais.

Não basta apenas estabelecer princípios éticos; é crucial implementá-los de maneira

prática e eficaz. Isso envolve criar estruturas que garantam a aderência contínua dos sistemas de IA a esses princípios durante todo o seu ciclo de vida (Bostrom, 2014).

Inclui medidas como: avaliação de impacto e conformidade, no qual antes de um sistema de IA ser implementado, deve haver uma avaliação rigorosa para identificar e mitigar potenciais impactos negativos sobre os direitos humanos e para o corpo social; transparência e explicabilidade: operações transparentes, e as decisões devem ser explicáveis para os usuários e afetados por elas; e, supervisão humana: especialmente aqueles em áreas de alto risco (Bostrom, 2014).

Assim, no atual estágio das discussões regulatórias, e em resposta às preocupações levantadas por pensadores como Bostrom, que o Parlamento Europeu tomou medidas significativas para estabelecer um marco regulatório para a IA (*AI Act*), visto que, aspirante ao protagonismo acerca de disciplina normativa da IA, definindo parâmetros deontológicos e programáticos com a finalidade de incentivar o desenvolvimento de soluções tecnológicas de IA em harmonia com a segurança de direitos e valores humanos (União Europeia, 2024).

As violações de direitos fundamentais decorrentes de desvios funcionais da IA residem, em grande parte, na opacidade e na complexidade algorítmica, permitindo que vieses inerentes nos dados sejam perpetuados e ampliados, resultando em discriminação. Para contrariar tais desvios, o *AI Act* impõe requisitos rigorosos de transparência e prestação de informações aos responsáveis pela implantação (operadores) de sistemas de IA de alto risco (União Europeia, 2024).

Esses sistemas devem ser concebidos para que o operador possa interpretar os resultados e utilizar o sistema de forma adequada, sendo obrigatória a inclusão de instruções de utilização claras e acessíveis, que detalhem capacidades, limitações e riscos previsíveis (União Europeia, 2024).

O principal mecanismo para a proteção de direitos fundamentais em face dos desvios da IA de alto risco, especialmente quando se trata de organismos públicos ou entidades privadas prestadoras de serviços públicos, é a Avaliação de Impacto sobre os Direitos Fundamentais (FRIA) (Art. 27) (União Europeia, 2024).

Esta avaliação é obrigatória antes da implantação do sistema e deve identificar os riscos específicos de danos suscetíveis de afetar pessoas ou grupos. Ao exigir que o operador determine as medidas a serem tomadas em caso de materialização desses riscos, como mecanismos de supervisão humana e procedimentos de tratamento de queixas, o *AI Act* estabelece uma

arquitetura de responsabilização e gestão de riscos contínua (União Europeia, 2024).

Conclui-se, assim, que a legislação europeia busca institucionalizar a razão prática (Alexy, 2014) para garantir que a dignidade e a autonomia humanas não sejam sacrificadas em nome da eficiência tecnológica.

CONCLUSÃO

A presente pesquisa buscou desmistificar a percepção da Sociedade da Informação como um fenômeno meramente técnico, revelando-a como uma nova estrutura de poder e acumulação. A Inteligência Artificial, por sua vez, emerge como o motor dessa transformação, atuando não apenas como uma ferramenta de processamento de dados, mas como um elemento central na consolidação de uma nova ordem social.

Nessa senda, a IA está na vanguarda das inovações tecnológicas, trazendo consigo a promessa de avanços significativos em diversas áreas, incluindo a vida cotidiana dos cidadãos, o mundo dos negócios e a administração pública. Seu potencial transformador é inegável, oferecendo novas soluções e melhorias que podem otimizar processos, aumentar a eficiência e criar oportunidades inéditas.

No entanto, essa mesma tecnologia que possibilita progressos também acarreta riscos consideráveis, tanto para a segurança dos usuários quanto para a preservação dos direitos fundamentais. A investigação das violações de direitos fundamentais por desvios funcionais da IA revelou que o viés algorítmico e a falta de transparência não são falhas isoladas, mas reflexos da subordinação da ética e da justiça à eficiência tecnológica.

Os sistemas de IA são intrinsecamente complexos e muitas vezes operam de maneira opaca. Sua autonomia e a dependência de grandes volumes de dados para treinamento e operação levantam preocupações sobre confiabilidade e segurança jurídica.

A pesquisa demonstrou que a proteção jurídica, se limitada a remédios *ex post*, é insuficiente contra os riscos de decisões automatizadas. O Regulamento da Inteligência Artificial da União Europeia, ao adotar uma abordagem baseada no risco e na ética, representa um marco regulatório essencial para promover a segurança, a confiança e o respeito pelos direitos fundamentais na União.

A imposição de requisitos rigorosos em matéria de governação de dados, transparência, solidez e supervisão humana, juntamente com a obrigatoriedade da Avaliação de Impacto sobre

os Direitos Fundamentais para usos específicos, configura uma arquitetura preventiva e de responsabilização algorítmica. Esta regulamentação assegura que, mesmo nos domínios mais sensíveis, como o emprego, a gestão de infraestruturas críticas ou a aplicação da lei, o avanço tecnológico se mantenha em consonância com os valores constitucionais.

Foi nesse ponto que a Teoria Discursiva do Direito de Robert Alexy (2014) se mostrou indispensável. Ao defender que os direitos fundamentais são princípios que devem ser ponderados, e não simplesmente sacrificados em nome de interesses econômicos, a teoria de Alexy nos fornece um arcabouço para lutar por uma IA que respeite a dignidade e a autonomia humana.

Como hipótese preliminar, considera-se que a atual estrutura de proteção jurídica ainda é insuficiente para lidar com os riscos decorrentes do uso indiscriminado de dados por sistemas de IA, sendo necessário fortalecer mecanismos regulatórios, com vistas a assegurar a privacidade, a transparência algorítmica e a não discriminação.

A privacidade e a proteção de dados na era da Inteligência Artificial não são questões que podem ser resolvidas com meras regulamentações superficiais. Elas exigem uma redefinição profunda dos conceitos jurídicos e uma luta contínua pela proteção da autodeterminação informativa. O futuro da Sociedade da Informação dependerá da nossa capacidade de garantir que a tecnologia, em vez de se tornar uma nova fonte de opressão, sirva como uma ferramenta para a emancipação e a realização dos direitos humanos.

Os avanços tecnológicos são inevitáveis, especialmente no contexto da Indústria 4.0, que está revolucionando a forma das interações. Em uma economia global cada vez mais interligada, a velocidade e a eficiência na disseminação de informações são impulsionadas por inovações tecnológicas, permitindo que as sociedades permaneçam funcionais mesmo em tempos de crise.

Nessa conjuntura torna-se claro que a gestão de categorias especiais de dados pessoais é circundada por uma série de obrigações legais que visam proteger a integridade e a privacidade dos indivíduos. O direito à privacidade e à proteção de dados pessoais tem de ser garantido ao longo de todo o ciclo de vida do sistema de IA.

Em última análise, a transparência algorítmica e a responsabilização legal emergem como pilares indispensáveis para a construção de uma IA de Confiança. O *AI Act* se posiciona como um catalisador para um novo regime de justiça, no qual a capacidade de fazer inferências deve estar sujeita aos princípios da proporcionalidade e do Estado de direito. A regulamentação demonstra o caminho para impedir que a eficiência tecnológica comprometa a autonomia e a

dignidade humana, garantindo que o futuro digital seja fundamentado no respeito integral pelos direitos dos cidadãos.

Tornando evidente que a evolução contínua da tecnologia exigirá regras mais detalhadas e modernas para enfrentar os novos desafios que surgem. Sendo necessário a criação de normas específicas para assegurar que os direitos fundamentais sejam protegidos de forma robusta, enquanto se fomenta um cenário que incentive a inovação ética e responsável em tecnologias de IA.

REFERÊNCIAS

ALEXY, Robert. **Teoria Discursiva do Direito.** Tradução de Alexandre Travessoni Gomes Trivisonno. Rio de Janeiro: Forense Universitária, 2014.

ASSMANN, Hugo. "**A metamorfose do aprender na sociedade da informação**". Disponível em: < https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://www.scielo.br/j/ci/a/ShzKdLbqJDPfssvSw9xWPrw/%3Fformat%3Dpdf%26lang%3Dpt&ved=2ahUKEwi5ufX09f6GAxX6rJUCHRYABksQFnoECBAQAQ&usg=AOvVaw0OboUAZM6dKDa_EGs-ONY9 >. Ci. Inf., Brasília, v. 29, n. 2, 2000. Acesso em 25 de abril de 2024.

ARMBRUST, Michel. FOX, Armando. A **view of cloud computing. Communications of the ACM**. 2010.

BELEZA, Gabriel Pinheiro. "**A PROTEÇÃO E O TRATAMENTO DE DADOS PESSOAIS POR SISTEMAS DE IA: UMA POSSIBILIDADE DE APLICAÇÃO ANALÓGICA DA LEI 13.709/18**" Disponível em: < https://bdm.unb.br/bitstream/10483/29391/1/2021_GabrielPinheiroBeleza_tcc.pdf >. Acesso em 05 de maio de 2024.

BENGIO, Youshua. **Learning Deep Architectures for AI**. Foundations and Trends in Machine Learning, e. Now Publishers, 2014.

BIONI, Bruno. "**Proteção de Dados Pessoais: A Função e os Limites do Consentimento**". Disponível em: < https://bibliotecadigital.tse.jus.br/xmlui/handle/bdtse/5973 >. Acesso em 26 de maio de 2024.

BURCH, Sally. "**Sociedade da informação/ Sociedade do conhecimento**" Disponível em: < https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://dcc.ufrj.br/~jonathan/compsoc/Sally%2520Burch.pdf&ved=2ahUKEwiavNft8P6GAxVps5UCHdYWATYQFnoECA8QAQ&usg=AOvVaw24adXW-Mi95IGrpRvpBvmr >. Acesso em 19 de março de 2024.

BRUNO, Fernanda *et al*. **Tecnopolíticas da Vigilância: Perspectivas da Margem**. São Paulo: Boitempo, 2018.

CASTELLS, Manuel. **A era da informação: economia, sociedade e cultura**. In: A Sociedade em rede. São Paulo : Paz e Terra, V.1, 2020.

CAPGEMINI RESEARCH INSTITUTE. Consumer and Business Insights: Artificial Intelligence in Daily Life. 2020. Disponível em: https://www.capgemini.com/insights/expert-perspectives/what-will-artificial-intelligence-bring-in-2020/. Acesso em: 28 set. 2025.

CEBRIÁN, Juan Luis. **A Rede: com o nossas vidas serão transformadas pelos novos meios de comunicação**. Lisboa: Summus, 1999.

DAVENPORT, Thomas. PRUSKA, Laurence. **Working Knowledge: How Organizations Manage What They Know**. Harvard Business School Press. 1998.

GOODFELLOW, Ian. BENGIO, Yoshua. COURVILLE, Aaron. ***Deep Learning***. MIT Press. 2016.

PROVOST, Foster. FAWCETT, Tom. **Data Science for Business: What You Need to Know About Data Mining and Data-Analytic Thinking**. O'Reilly Media. 2016.

HARARI, Yuval Noah. Homo Deus. Uma breve história do amanhã. São Paulo: Companhia das Letras, 2016.

FLORIDI, Luciano. SANDERS, J. W. **On the morality of artificial agents**. *M*inds and Machines, 14(3), 2004.

RODOTA, Stefano. "**A Vida na Sociedade da Vigilância**". Renovar, 2017.

REQUIÃO, Maurício; COSTA, Diego Carneiro. Discriminação algorítmica: ações afirmativas como estratégia de combate. Civilistica.com, ano 11, n. 3, 2022. Disponível em <https://civilistica.emnuvens.com.br/redc/article/view/804 >. Acesso em 04 out. 2025.

RUSSELL, Stuart. NORING, Peter. **Artificial Intelligence: A Modern Approach.** Prentice Hall. 2020.

SILVA, Alexandre Assunção. **Sigilo das Comunicações na Internet**. Curitiba: Juruá Editora, 2017.

ZUBOFF, Shoshana. **The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power**. Nova York: PublicAffairs, 2019.