ABORDAGENS TEÓRICAS E PRÁTICAS EM PESQUISA

COORDENADORES

Patricia Bieging

Raul Inácio Busarello

ISBN 978-85-7221-591-6

2026

Jardson Ferreira da Silva

Mara Augusto Dias

Mirella Fernandes Atanázio

Rodrigo Murad Vitoriano

O BIG DATA E SUAS IMPLICAÇÕES NO ORDENAMENTO JURÍDICO NACIONAL

DOI: 10.31560/pimentacultural/978-85-7221-591-6.2

RESUMO:

Atualmente cada vez mais se tem falado em Big Data, ou seja, os grandes volumes de dados, estruturados ou não, em alta velocidade e variedade, que buscam extrair informações relevantes, sendo certo que no ordenamento jurídico nacional seu impacto é cada vez mais expressivo. Na seara do Direito, tal ferramenta pode ser aplicada na gestão de pessoas, na análise preditiva, no compliance e investigação e ainda em políticas públicas. Entretanto, em que pese sua importância, há muitos desafios a serem enfrentados, sobretudo em questões ligadas à transparência e ética, proteção de dados pessoais, segurança da informação e conflitos com os direitos fundamentais. Neste contexto, o presente artigo busca delinear aspectos desta importante inovação tecnológica, em benefício da coletividade, utilizando-se, para tanto, de metodologia de pesquisa bibliográfica e abordagem qualitativa, com base na análise da doutrina, da legislação e de estudos sobre o tema.

Palavras-chave: big data; volume de dados; desafios; transparência; ética; proteção; segurança da informação; direitos fundamentais.

ABSTRACT:

Nowadays, there is increasing discussion about Big Data, that is, large volumes of data, structured or unstructured, with high velocity and variety, which aim to extract relevant information. It is evident that, within the national legal framework, its impact is becoming increasingly significant. In the field of Law, such a tool can be applied in human resources management, predictive analysis, compliance and investigation, as well as in public policies. However, despite its importance, many challenges remain, especially regarding transparency and ethics, personal data protection, information security, and conflicts with fundamental rights. In this context, the present article aims to outline aspects of this important technological innovation for the benefit of society, using, for this purpose, a bibliographic research methodology and a qualitative approach, based on the analysis of doctrine, legislation, and studies on the subject.

Keywords: *big data; data volume; challenges; transparency; ethics; protection; information security; fundamental rights.*

INTRODUÇÃO

A contemporaneidade é inequivocamente moldada por avanços tecnológicos exponenciais, alçando o Big Data e a Inteligência Artificial (IA), protagonistas de uma nova era, frequentemente denominada Quarta Revolução Industrial. Tal fenômeno não se restringe a meras inovações técnicas, mas desencadeia uma transformação digital profunda e abrangente, impactando de forma indelével todas as esferas da sociedade, desde a economia, a cultura e as relações sociais, até o próprio universo jurídico, conforme destacado por Hoffmann-Riem (2020).

Referido fenômeno permite a emergência de sistemas ciberfísicos para novos processos de produção em rede e automatizados, altera a forma como as pessoas vivem as suas vidas e propicia a criação e utilização de redes sociais, além de fomentar novos serviços de comunicação e novos sistemas de vigilância por empresas privadas e agências governamentais (Hoffmann-Riem, 2020).

Neste sentido, o Direito, enquanto fato social dinâmico e instrumento de controle social, vê-se desafiado a interpretar, regulamentar e, por vezes, redefinir-se para dar conta dessa nova realidade, que, embora promissora em termos de otimização e eficiência, apresenta uma série complexa de dilemas éticos e jurídicos, exigindo do sistema legal uma revisão fundamental (Hoffmann-Riem, 2020).

Especificamente quanto ao Big Data, este refere-se a uma das manifestações mais significativas da era digital, caracterizando-se pela coleta, processamento e interpretação de quantidades massivas de dados, sejam eles estruturados ou não, em velocidade e escala inigualável. Nesta seara, o crescimento acelerado das capacidades tecnológicas de armazenamento e análise informacional repercute de maneira ampla em diferentes esferas da vida social, incluindo o setor jurídico.

Segundo preceituam Museti e Finoto (2023, p. 24):

> O Big Data pode ser considerado a coleta de um grande volume de dados, que vai desde o mais simples, como o nome e e-mail, até os mais complexos, como o endereço e etnia. Esses dados são coletados substancialmente por meio da internet, sendo armazenados e utilizados, muitas vezes, para direcionar conteúdos, anúncios, sites, entre outros, de acordo com o gosto pessoal de cada indivíduo.

Já para Douglas Eduardo Basso (2020), de uma forma mais simplificada, podemos dizer que Big Data é um conjunto de dados mais complexo e maior, utilizando uma gama de novas fontes, sendo que esses conjuntos de dados possuem grande volume, algo que softwares tradicionais de processamento de dados simplesmente não conseguem gerenciar.

Quanto à seara jurídica, o Big Data contribui para a otimização da gestão administrativa e processual, por meio do emprego de técnicas de análise preditiva, jurimetria e sistemas de inteligência artificial aplicados à prática forense. Entretanto, há também inúmeros desafios, como a garantia da privacidade, a proteção de dados pessoais, a salvaguarda da autodeterminação informativa e a mitigação de eventuais vieses discriminatórios embutidos em algoritmos.

Nesta conjectura, no Brasil estão em vigor algumas Leis importantes, como a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados – LGPD), que disciplina princípios e limites no tratamento de dados pessoais, e a Lei nº 12.965/2014 (Marco Civil da Internet), que busca assegurar a proteção da privacidade e a liberdade de expressão no ambiente digital.

Ainda, impende considerar que se debate com frequência a compatibilidade da utilização massiva de dados com a proteção dos direitos fundamentais inseridos expressa ou tacitamente na Constituição Federal de 1988, principalmente os princípios da dignidade da pessoa humana e da inviolabilidade da intimidade e da vida privada.

Ante o exposto, a análise das consequências jurídicas do Big Data e sua utilização pela Inteligência Artificial exige um olhar técnico e também uma avaliação crítica de natureza normativa e axiológica, a fim de garantir que o avanço tecnológico se desenvolva em harmonia com os princípios constitucionais, sobretudo o da integridade da pessoa humana, em benefício da sociedade.

Para esse fim, o presente estudo adota procedimentos metodológicos de pesquisa bibliográfica e abordagem qualitativa, fundamentando-se na análise da doutrina especializada, da legislação pertinente e de estudos contemporâneos sobre o tema. Essa metodologia permite uma compreensão aprofundada das implicações jurídicas, éticas e sociais da convergência entre Big Data e Inteligência Artificial, bem como a identificação de lacunas e desafios emergentes para o ordenamento jurídico.

O estudo, desenvolvido a partir dessa perspectiva, propõe-se a adentrar essa complexa intersecção, investigando os múltiplos impactos da convergência entre Big Data e IA no cenário jurídico, a partir da análise de livros e artigos científicos contemporâneos que abordam o tema. Será dada especial atenção aos desafios emergentes no que concerne à discriminação algorítmica, à proteção da privacidade e dos dados pessoais em um ambiente de coleta massiva de informações, à necessidade premente de transparência e *accountability* dos sistemas decisórios algorítmicos e à crescente concentração de poder no ecossistema digital. Ao fazê-lo, busca-se identificar as insuficiências do Direito tradicional face a essas inovações disruptivas, reafirmando que a Constituição permanece como um porto seguro para o jurista (Azevedo; Jahn, 2020).

BIG DATA E O DIREITO

Para compreender os desafios jurídicos, é essencial definir Big Data e IA e suas interconexões. Big Data se refere a conjuntos

de dados tão volumosos e complexos que exigem novas ferramentas para processamento e análise, caracterizados por Volume, Velocidade, Variedade, Veracidade e Valor (Hoffmann-Riem, 2020).

A Inteligência Artificial, por sua vez, é constituída por máquinas autônomas que percebem e raciocinam, frequentemente utilizando *machine learning*, que é o aprendizado por experiência e *deep learning*, caracterizado pelo aprendizado autônomo (Azevedo; Jahn, 2020, Hoffmann-Riem, 2020).

A sinergia entre Big Data e IA não apenas otimiza a análise de grandes volumes de informações, mas também cria um novo tipo de inteligência capaz de processar e aprender de formas sem precedentes, redefinindo as bases da interação humana e, consequentemente, do Direito.

A característica mais distintiva das tecnologias de Big Data e Inteligência Artificial, e uma das que mais profundamente impacta o Direito é sua operação intrínseca baseada na lógica indutiva, em contraste com a lógica dedutiva que historicamente fundamentou o pensamento jurídico e científico ocidental. Pugliesi e Brandão (2015) oferecem uma análise detalhada dessa distinção: enquanto a lógica dedutiva, conforme a tradição cartesiana, busca a certeza na qual a verdade das premissas garante a verdade da conclusão, a lógica indutiva trabalha com a noção de probabilidade e correlações.

Em um argumento dedutivamente válido, as asserções de ordem factual estão encerradas nas premissas, tornando impossível uma conclusão falsa se as premissas são verdadeiras (Pugliesi; Brandão, 2015). Assim, conclusão não extravasa o que está contido nas premissas.

Por outro lado, a lógica indutiva, central para o Big Data, lida com a probabilidade indutiva, no qual as premissas oferecem algum apoio para a conclusão, mas não a asseguram completamente. A conclusão, nesse caso, extravasa as asserções contidas nas premissas,

permitindo a previsão e a descoberta de fatos novos a partir de dados conhecidos, mesmo com o risco de erro. Com isso, a capacidade de encontrar pequenos padrões ou correlações em um oceano de complexidade de dados, com a finalidade de extrair informações úteis, é o ponto nevrálgico do Big Data (Pugliesi; Brandão, 2015).

A rápida evolução das tecnologias digitais tem conduzido os algoritmos de Big Data a operarem com algoritmos indutivos, no qual a indução, nas ciências da computação, frequentemente diz respeito à aplicação do princípio da recorrência a gráficos. Essa lógica indutiva de dados inverte certos parâmetros da lógica dedutiva de dados, resultando em premissas como esquecer mais dados para mais possibilidades e procurar por singularidades e desconhecidos (Pugliesi; Brandão, 2015).

Ainda, a análise de grandes volumes de dados prioriza a velocidade em detrimento da certeza, pois, como apontam Pugliesi e Brandão (2015), uma informação correta, ainda que arriscada no momento, é preferível a outra totalmente confiável tempos depois, especialmente na contemporaneidade, em que cada segundo conta no mercado da vida.

Essa transição paradigmática para uma lógica indutiva de dados desafia as próprias bases do Direito. Se o sistema legal se estrutura em torno de princípios de causalidade, previsibilidade e certeza jurídica, a lógica indutiva, com sua ênfase em correlações e probabilidades, introduz uma imperfeição e um dinamismo que o Direito deve absorver (Pugliesi; Brandão, 2015).

A capacidade de prever o futuro e de guiar ações a partir de padrões, mesmo imperfeitos, exige do Direito uma nova postura, questionando se as regras jurídicas tradicionais são adequadas para fazer justiça à problemática da situação em transformação e para implementar novos valores-alvo sob as novas condições. Neste sentido, a aplicação do Big Data e da IA gera desafios que exigem uma

profunda reavaliação do Direito, pois essas tecnologias influenciam decisões e comportamentos de formas que o arcabouço jurídico tradicional não conseguiria sequer imaginar (Hoffmann-Riem, 2020).

DESAFIOS JURÍDICOS NA ERA DO BIG DATA E DA INTELIGÊNCIA ARTIFICIAL

A aplicação generalizada de Big Data e Inteligência Artificial nas mais diversas esferas da vida social e econômica tem gerado um conjunto de desafios jurídicos fundamentais, que exigem uma reavaliação profunda dos institutos e princípios que historicamente pautaram o Direito. Tais desafios emergem da capacidade sem precedentes dessas tecnologias de coletar, processar e analisar informações em escala massiva, influenciando decisões e comportamentos de maneiras que o arcabouço jurídico tradicional, como já cediço, não foi concebido para abarcar eficaz e plenamente (Hoffmann-Riem, 2020).

A utilização de sistemas de IA e Big Data em processos de decisão automatizada, como o recrutamento e seleção de pessoal, embora justificada pela busca de eficiência, introduz um risco latente e complexo de discriminação algorítmica. Azevedo e Jahn (2020) destacam que tais ferramentas possuem um potencial considerável de promover atos discriminatórios, demandando uma atenção redobrada por parte do jurista.

O Cenário da Discriminação Pré-Contratual no Âmbito Laboral

A discriminação, em sua acepção jurídica, é conceitualmente definida por Azevedo e Jahn (2020) como todas as diferenciações, exclusões ou restrições vivenciadas por alguns grupos que tenham por fim, ou por efeito, impedir ou dificultar o reconhecimento, o desfrute ou o exercício de direitos usuais da vida em sociedade, em igualdade de condições com terceiro.

As normas de Direito da Antidiscriminação buscam evitar que certas características pessoais, frequentemente associadas a qualidades de inferioridade social, venham a ensejar uma considerável redução das possibilidades de exercício das suas potencialidades sociais (Azevedo; Jahn, 2020).

O ordenamento jurídico brasileiro é robusto nesse combate, pois a Constituição Federal de 1988 elenca a rejeição à discriminação como um objetivo fundamental da República (art. 3º, inc. IV), consagra o princípio da igualdade (art. 5º, *caput*) e prevê a punição de qualquer discriminação atentatória dos direitos e liberdades fundamentais (art. 5º, inc. XLI).

No âmbito juslaboral, essa proteção também é reforçada, uma vez que o art. 7º da Constituição Federal, em seus incisos XXX, XXXI e XXXII, veda expressamente a diferença de salários, de exercício de funções e de critérios de admissão baseados em deficiência, sexo, idade, cor ou estado civil, bem como a distinção entre funções ou profissões (Azevedo; Jahn, 2020). Já a Consolidação das Leis do Trabalho, desde seu texto original, estabelece o princípio da igualdade salarial (art. 5º).

A Lei n. 9.029/1995 proibiu a exigência de atestado de estado gravídico ou esterilização e vedou a dispensa discriminatória, com a Súmula n. 443 do Tribunal Superior do Trabalho, presumindo-a em casos de doenças que suscitem estigma ou preconceito (Azevedo; Jahn, 2020).

Mais tarde, a Lei n. 9.799/1999, ao incluir o art. 373-A à CLT, arrolou uma série de vedações, como a proibição de anúncios de emprego com referências discriminatórias ou a recusa de emprego baseada em características protegidas, salvo exceções estritamente ligadas à natureza da atividade (Azevedo; Jahn, 2020). Embora essa legislação seja abrangente, Azevedo e Jahn (2020) apontam que a discriminação é mais recorrente na fase pré-contratual, momento em

que o empregador exerce o poder de escolha, e nesta fase o trabalhador se encontra em estágio de grande vulnerabilidade.

A Reprodução de Vieses Através da Publicidade Direcionada e dos Algoritmos de Triagem

Nesta seara, a preocupação com a discriminação algorítmica reside na capacidade das novas tecnologias de reproduzir e até amplificar vieses humanos existentes, muitas vezes de forma sutil e indireta. Azevedo e Jahn (2020), baseando-se em Pauline Kim, apontam dois mecanismos principais nos processos de admissão de novos empregados que são suscetíveis a isso, sendo o primeiro deles, a publicidade direcionada de vagas em redes sociais.

Embora as mídias sociais possuam um vasto rol de dados sobre seus usuários, permitindo uma segmentação precisa, o risco é que empregadores podem usar essas ferramentas para deliberadamente excluir ou atingir determinados grupos (Azevedo; Jahn, 2020).

A segmentação pode ocorrer de forma indireta, por meio de dados como localização, preferências, curtidas ou comunidades, que podem indicar, por exemplo, o gênero, etnia, faixa etária ou estado gravídico do usuário, burlando as proibições legais do art. 373-A da CLT (Azevedo; Jahn, 2020).

O segundo mecanismo é constituído por algoritmos de triagem e pontuação de currículos, que são utilizados para prever quais candidatos terão melhor desempenho no trabalho, operando de modo a buscar correlações estatísticas entre variáveis e utilizando experiências passadas para construir padrões (Azevedo; Jahn, 2020).

Contudo, a utilização desse mecanismo, segundo Azevedo e Jahn (2020), pode resultar em erros ou vieses significativos, podendo vir a ocorrer perda de oportunidades de emprego por razões absolutamente arbitrárias. Pode-se citar, como exemplo, a discriminação étnica

que pode ocorrer indiretamente pelo Código de Endereçamento Postal (CEP), em que algoritmos, ao analisarem dados sociodemográficos de determinadas localidades, podem inferir características que levam à discriminação de uma comunidade vulnerável, mesmo que o CEP em si não contenha juízo de valor (Azevedo; Jahn, 2020).

A suposta neutralidade das máquinas, frequentemente defendida, é desmistificada, pois as máquinas não estariam sujeitas às imperfeições humanas e toda a parcialidade decorrente das experiências de vida. Todavia, a ciência dos algoritmos tem o objetivo de detectar padrões nos dados para fazer previsões futuras que nem sempre representam a realidade. A versão criada pelo algoritmo inclui possíveis vieses humanos e preconceitos refletidos nos dados, no algoritmo ou no modelo aprendido (Azevedo; Jahn, 2020).

Dessa forma, um algoritmo treinado com dados de contratações passadas de uma empresa que privilegiava um determinado perfil tenderá a reproduzir os vieses anteriormente existentes, perpetuando a exclusão de grupos (Azevedo; Jahn, 2020). Esse fenômeno evidencia como decisões automatizadas podem reforçar desigualdades sociais, mesmo quando não há intenção explícita de discriminação por parte da organização.

O Desafio da Fiscalização na Nova Realidade Algorítmica

A forma como a discriminação ocorre na era digital torna sua fiscalização consideravelmente mais complexa do que no passado. Azevedo e Jahn (2020) pontuam que, se no modelo tradicional, um anúncio discriminatório em um jornal permitia que o grupo prejudicado tomasse ciência e buscasse as medidas cabíveis, na publicidade digital direcionada, a fiscalização da prática discriminatória provocada através de algoritmos é dificultada, pois o grupo excluído nem sequer terá acesso ao anúncio, pois a estes a publicação não será direcionada. Essa invisibilidade impede a denúncia e a atuação de órgãos de fiscalização, como o Ministério Público do Trabalho.

Além disso, a capacidade de *machine learning*, que em tese permitiria aos algoritmos corrigir eventuais falhas, mostra-se limitada no contexto das relações de emprego. Isso ocorre porque o *feedback* necessário para o aprendizado do modelo nem sempre se materializa. Se um algoritmo classifica candidatos como não qualificados de forma equivocada, esses indivíduos não serão contratados e o empregador dificilmente será constatado de que houve um erro, resultando na perpetuação dos erros e vieses no modelo (Azevedo; Jahn, 2020).

Por tais razões, a implementação da inteligência artificial e big data para a contratação de empregados demanda atenção e cuidado, com as mesmas preocupações que ensejaram a edição das normas de Direito da Antidiscriminação (Azevedo; Jahn, 2020), exigindo uma constante revisão e atualização da abordagem jurídica.

A PROTEÇÃO DA PRIVACIDADE E DOS DADOS PESSOAIS: DO CONSENTIMENTO À ILUSÃO DE CONTROLE

A privacidade, um direito fundamental e um valor inalienável em qualquer sociedade democrática, consagrado no art. 5º, inciso X, da Constituição Federal, enfrenta um desafio sem precedentes com o avanço e a proliferação do Big Data. Pugliese e Brandão (2015) destacam que, embora a preocupação com a invasão da privacidade não seja um fenômeno novo, remetendo a figuras como Warren e Brandeis no final do século XIX, a sociedade de informação e controle atual exacerba dramaticamente o problema, marcada por um constante controle de informação e a geração de volumes massivos de dados, com mais de 2,4 bilhões de usuários de internet no mundo (Pugliesi; Brandão, 2015).

O arcabouço legal da proteção de dados, exemplificado pelo Regulamento Geral de Proteção de Dados (GDPR) da União Europeia, que serviu de inspiração para a Lei Geral de Proteção de Dados (LGPD) no Brasil, se estrutura fundamentalmente sobre

o conceito de consentimento como base legal para o tratamento de dados pessoais.

O art. 4º, n. 11, do GDPR define consentimento como uma manifestação de vontade, livre, específica, informada e explícita, aceita pelo titular dos dados mediante declaração ou ato positivo inequívoco (Hoffmann-Riem, 2020). A efetividade desse consentimento é profundamente questionada.

Hoffmann-Riem (2020) problematiza a voluntariedade do consentimento (art. 7º, nº 4, GDPR), especialmente quando a execução de um serviço está condicionada à aceitação de termos que incluem o tratamento de dados não essenciais para a prestação do serviço principal. Ele argumenta que, em cenários nos quais determinados serviços são indispensáveis aos usuários, seja por razões profissionais ou pessoais importantes e quando não houver ofertas concorrentes de qualidade comparável, este público se desloca para uma posição em que não há outra alternativa senão dar o seu consentimento (Hoffmann-Riem, 2020). Referida situação configura uma notória ausência de paridade contratual, em que o consentimento, embora formalmente dado, carece de genuína voluntariedade.

Os Princípios de Proteção de Dados

Os princípios basilares da proteção de dados, como a limitação da finalidade e a minimização de dados (art. 5º, parágrafo 1, GDPR), que visam restringir a coleta e o uso de dados ao estritamente necessário para propósitos específicos, enfrentam sérias dificuldades de aplicação no contexto do Big Data.

Hoffmann-Riem (2020) explica que, para dados agregados, é comum que as informações de origem sejam utilizadas para vários fins e que nem sempre é possível, no momento do consentimento do titular dos dados, identificar que informação deve ser gerada pelo tratamento no domínio dos grandes volumes de dados e qual o seu

significado. Além disso, os objetivos da utilização subsequente dos dados frequentemente não são claros, o que esvazia a exigência da finalidade pretendida.

A natureza do Big Data, que opera com a premissa de que quanto mais dados de diferentes tipos estiverem disponíveis, mais bem-sucedida é, em princípio, a análise de Big Data, contradiz diretamente o princípio da minimização. Isso conduz as empresas a criticarem a relevância desses princípios para as aplicações de Big Data, argumentando que eles seriam um obstáculo e uma inibição da inovação (Hoffmann-Riem, 2020). No entanto, a doutrina ressalta que o abandono desses princípios não se justifica, pois eles são essenciais para a proteção de interesses jurídicos fundamentais e para a observância da proporcionalidade.

Neste sentido, a proteção não pode limitar-se apenas aos dados pessoais, mas deve se estender a dados industriais e a outras consequências sociais da digitalização, pois o Regulamento Geral de Proteção de Dados, por exemplo, é considerado insuficiente nesse aspecto (Hoffmann-Riem, 2020).

A profundidade dos impactos do Big Data sobre a privacidade e a autonomia individual é revelada pelos três paradoxos do Big Data. Segundo Pugliesi e Brandão (2015), o primeiro é o paradoxo da transparência, no qual o Big Data promete conhecer mais o mundo, deixá-lo mais transparente, mas, promove coletas invisíveis, utilizando ferramentas opacas, rodeadas de mistério. A questão fundamental que emerge é: Se big data traz o fim da privacidade, porque a revolução de big data está acontecendo em sua maior parte em segredo? (Pugliesi; Brandão, 2015).

A conclusão que se extrai é que a falta de visibilidade impede o controle e a responsabilização, tornando a fiscalização extremamente difícil (Hoffmann-Riem, 2020). Ainda, ao mesmo tempo em que busca identificar, por meio do paradoxo da identidade, o Big Data ameaça a identidade individual. Isto porque, em democracias liberais, há o direito

de escolha sobre identidade, mas a combinação de vastos dados (telefônicos, histórico de internet, compras, redes sociais) permite que a IA construa perfis tão precisos que a escolha de identidade se torne uma imposição. O eu sou se torna você é, e o eu gosto se torna você gosta, transformando a identidade de uma construção pessoal para uma determinação algorítmica (Pugliesi; Brandão, 2015).

Hoffmann-Riem (2020) aduz que o paradoxo da identidade atribuída ao Big Data levanta preocupações sobre a autonomia e a autodeterminação, pois os indivíduos podem ser tratados com base em características atribuídas a um determinado grupo sem que tenham sido efetuadas inquirições a este respeito, afetando áreas como saúde, recursos financeiros ou até mesmo orientação sexual.

Por último, o Big Data é apresentado como uma tecnologia que beneficia a todos, mas, na realidade, aumenta o poder de organizações sobre os indivíduos, que têm seus dados constantemente minerados, analisados e agrupados, desaguando no que Pugliesi e Brandão (2015) denominam de paradoxo de poder.

A dinâmica instaurada pelo Big Data cria um incerto estado de coisas que não é saudável para ninguém e deixa direitos dos indivíduos em erosão e nossa democracia diminuída. Os riscos incluem *profiling*, *tracking*, discriminação, exclusão e vigilância governamental, com consequente perda de controle por parte dos indivíduos. A penumbra da tecnologia, sem claras limitações legais e opacas limitações técnicas (Pugliesi; Brandão, 2015), faz com que indivíduos e instituições operem em terreno movediço, sem controle efetivo sobre as consequências do uso massivo de dados.

TRANSPARÊNCIA E ACCOUNTABILITY ALGORÍTMICA

A complexidade inerente e a natureza frequentemente opaca dos sistemas algorítmicos, especialmente aqueles que se baseiam em técnicas de *machine learning* e *deep learning*, criam ainda um

desafio significativo para a transparência e a accountability. A incapacidade de compreender os critérios e a lógica envolvida nas decisões automatizadas impede o controle efetivo, seja por parte dos indivíduos afetados, das autoridades reguladoras ou do público em geral (Hoffmann-Riem, 2020).

Tanto a Lei Geral de Proteção de Dados (LGPD) no Brasil (art. 20, § 1º) quanto o Regulamento Geral de Proteção de Dados (GDPR) na Europa (art. 13, 14 e 22) tentam endereçar o problema da opacidade algorítmica ao prever o direito de explicação. Com isso, o direito de explicação permite que o titular dos dados exija informações sobre os critérios e procedimentos utilizados em decisões automatizadas que o afetem, servindo como um mecanismo crucial para a fiscalização de potenciais vieses discriminatórios (Azevedo; Jahn, 2020).

Ao discutir o direito de explicação em face de decisões automatizadas, Azevedo e Jahn (2020) enfatizam sua legitimidade quando há suspeita de o algoritmo estar se valendo de informações proibidas para tomar suas decisões, como no caso hipotético de considerar a etnia do candidato para decidir sobre o seu acesso ao emprego. Nesse caso, o empregador ou fornecedor da tecnologia teria o ônus de provar que o modelo é válido e que as características consideradas são substantivamente significativas, não bastando uma alegação genérica de relação com o trabalho (Azevedo; Jahn, 2020).

No entanto, Hoffmann-Riem (2020) aponta falhas no direito de explicação, aferindo que os usuários ficam sobrecarregados com montanhas de dados, que, aliás, contêm muitas abreviaturas e termos que são amplamente desconhecidos, de modo que informações significativas só podem ser obtidas, de fato, por especialistas. As próprias autoridades de proteção de dados, por sua vez, também enfrentam problemas de informação consideráveis para fiscalizar como as empresas usam Big Data e sua análise.

Com isso, temos que a falta de transparência é, em grande parte, uma escolha estratégica de muitas empresas do setor de TI.

Hoffmann-Riem (2020) observa que várias empresas evitam tanto quanto possível a transparência, excluem em grande medida a possibilidade de terceiros reproduzirem os procedimentos e, assim, impedem oportunidades para um controle externo eficaz. Essa postura corporativa é frequentemente justificada pela proteção de segredos comerciais, o que, embora legítimo, não pode ser um escudo absoluto contra a fiscalização de práticas que possam prejudicar interesses jurídicos fundamentais ou o interesse público.

A situação se agrava ainda mais com os algoritmos de aprendizado (como *deep learning*), nos quais mesmo os desenvolvedores e programadores podem perder a transparência dos processos, gerando um problema da falta de controlabilidade humana do desenvolvimento autodirigido dos programas, no qual as possibilidades de supervisão humana ou mesmo de contrariar acontecimentos ou catástrofes indesejáveis são dificultadas ou mesmo eliminadas (Hoffmann-Riem, 2020).

A perda de controle no que concerne à transparência dos processos, que não se restringe apenas à superfície da comunicação, mas abrange o conhecimento do funcionamento dos algoritmos, compromete a base para a responsabilização por decisões automatizadas de alto impacto.

Hoffmann-Riem (2020) enfatiza que a transparência é um pré-requisito para garantir, em particular, a responsabilização. A ausência dessa transparência eficaz resulta em um déficit de *accountability*, no qual a atribuição de culpa e a correção de erros se tornam nebulosas, gerando preocupações sobre as decisões institucionais tomadas com o auxílio de Big Data (Pugliesi; Brandão, 2015).

BIG DATA, INTELIGÊNCIA ARTIFICIAL E A VIGILÂNCIA ESTATAL

O uso de Big Data e Inteligência Artificial não se restringe ao setor privado, sendo cada vez mais empregado por autoridades

públicas para fins de vigilância, segurança e controle, levantando questões jurídicas complexas sobre o equilíbrio entre a segurança coletiva e as liberdades individuais. As medidas de vigilância estatal, por exemplo, pela polícia ou pelos serviços de informações, são também controladas por algoritmos (Hoffmann-Riem, 2020).

A doutrina destaca a aplicação proativa e reativa de Big Data na vigilância estatal, como no conceito de policiamento preditivo. Isso ocorre pela capacidade de coletar e analisar vastos volumes de dados para registrar tendências de desenvolvimento e permitir novos tipos de produção e distribuição, bem como tarefas do Estado (Hoffmann-Riem, 2020).

No contexto europeu, embora não seja diretamente aplicável ao Big Data de forma abrangente, a Diretiva (UE) 2016/680 trata da proteção de dados pessoais pelas autoridades competentes para fins de prevenção e repressão de infrações penais. No entanto, Hoffmann-Riem (2020) ressalta que essa diretiva e sua transposição excluem os problemas regulamentares especiais com os megadados, mesmo que esses sejam utilizados em segurança.

Os problemas de falta de transparência e *accountability*, já observados no setor privado, também se manifestam no campo do direito público. Assim, ainda que a vigilância estatal seja dependente do sigilo, não há isenção das obrigações legais para o Poder Público. Hoffmann-Riem (2020) defende a importância de se construir disposições eficazes de controle pelos tribunais, parlamentos e o público, especialmente porque a proteção judicial pode ser limitada ou confiada a organismos de controle específicos.

Ainda, o desenvolvimento da digitalização e o uso de Big Data estão associados a riscos que podem colocar em perigo a cibersegurança, como a funcionalidade dos sistemas de TI e, crucialmente, das infraestruturas críticas, as quais podemos citar os hospitais, energia e transporte. Tais riscos incluem vulnerabilidades em

hardware e *software* e ciberataques direcionados, que podem visar desde a desinformação e manipulação (exemplo, de eleições), até a sabotagem (Hoffmann-Riem, 2020).

Paradoxalmente, a doutrina aponta a natureza bilateral do Big Data e da IA. Neste sentido, embora possam ser ferramentas para ataques, oferecem também um ponto de partida para melhorar a segurança das próprias tecnologias de informação. A análise de Big Data, por exemplo, permite a detecção e combate de um ataque a sistemas de TI ou processos de comunicação individuais e a identificação de padrões de atividade que representam uma ameaça (Hoffmann-Riem, 2020).

A Diretiva (UE) 2016/1148 (Diretiva NIS) é um exemplo de esforço regulatório para garantir um alto nível comum de segurança das redes e sistemas informáticos na União Europeia, impondo obrigações aos Estados-Membros e aos operadores de serviços essenciais. No entanto, a cibersegurança não é apenas um problema nacional, mas um desafio transnacional e internacional (Hoffmann-Riem, 2020).

É crucial, contudo, que o aumento das capacidades de vigilância e segurança do Estado seja acompanhado de um controle rigoroso. Hoffmann-Riem (2020) argumenta que a efetividade da vigilância não justifica a ausência de obrigações legais e de controle. A expansão da proteção contra a vigilância do Estado é fundamental, especialmente no que se refere ao policiamento preditivo e deve incluir sanções para infrações.

A análise desenvolvida demonstra que o avanço do Big Data e da Inteligência Artificial inaugura um ambiente em que os institutos jurídicos tradicionais já não oferecem respostas plenamente adequadas. Assim, a lógica probabilística que orienta essas tecnologias tensiona noções clássicas como previsibilidade, causalidade e estabilidade normativa, ao mesmo tempo em que gera efeitos concretos em

diversas frentes: amplifica riscos de discriminação algorítmica nos processos seletivos, enfraquece a autonomia e a privacidade diante da coleta massiva e pouco transparente de dados, dificulta o exercício da transparência e da responsabilização e amplia as capacidades estatais de vigilância sem garantias democráticas proporcionais.

Diante desse panorama, impõe-se ao Direito a tarefa de desenvolver soluções regulatórias mais sofisticadas e coerentes com a realidade digital, capazes de equilibrar inovação, proteção de direitos fundamentais e mecanismos de controle efetivo, sob pena de permitir que a transformação tecnológica aprofunde desigualdades e fragilize a própria ordem democrática.

DESAFIOS:
A QUESTÃO DA ÉTICA E TRANSPARÊNCIA E OS DIREITOS FUNDAMENTAIS

O Big Data configura-se como uma ferramenta promissora para a pesquisa e a inovação, possibilitando novas descobertas e soluções em diferentes áreas do conhecimento. Contudo, o processamento de um volume massivo de dados pode gerar instabilidades significativas, especialmente no que se refere à segurança da informação, à confiabilidade dos resultados e à proteção da privacidade dos indivíduos.

Florea e Florea (2020) destacam que, embora o Big Data ofereça uma promessa valiosa para a pesquisa e inovação, ele também representa um risco considerável à privacidade, exigindo uma revisão das políticas e práticas atuais de proteção de dados. Atualmente, observa-se um grande impacto decorrente do crescente volume de dados coletados, resultado da intensa circulação de informações adquiridas por empresas e órgãos públicos. Muitas vezes, porém,

não há transparência quanto à forma como esses dados são utilizados, o que gera incertezas e preocupações quanto à proteção da privacidade e ao respeito aos direitos fundamentais.

PROTEÇÃO DE DADOS PESSOAIS

A proteção de dados pessoais configura-se como um dos principais desafios da sociedade digital, especialmente diante do volume crescente de informações coletadas por empresas e órgãos públicos. A Lei Geral de Proteção de Dados (LGPD) estabelece princípios como finalidade, adequação e necessidade, delimitando os limites para o tratamento de informações.

Assim, a proteção de dados deve ser entendida como uma garantia fundamental, vinculada diretamente à preservação da dignidade da pessoa humana e ao exercício pleno da cidadania. Nesse contexto, é importante destacar que a própria LGPD, em seu artigo 6º, estabelece que o tratamento de dados deve observar princípios como a finalidade específica, a necessidade da coleta, a transparência e a segurança, de modo a assegurar não apenas o uso legítimo das informações, mas também a proteção contra abusos. Tais diretrizes reforçam a compreensão de que a privacidade e a autodeterminação informativa não se configuram apenas como interesses individuais, mas como direitos fundamentais indispensáveis à consolidação do Estado Democrático de Direito.

TRANSPARÊNCIA ÉTICA

A utilização de algoritmos em processos de tomada de decisão demanda ainda uma abordagem ética pautada pela transparência. A ausência de clareza quanto aos critérios utilizados em sistemas automatizados pode resultar em decisões discriminatórias e de difícil contestação, prejudicando a confiança dos cidadãos.

A legislação já prevê o direito de revisão de decisões automatizadas, demonstrando a preocupação em assegurar que a inovação tecnológica não comprometa a igualdade de tratamento e a justiça social. Essa previsão normativa permite que indivíduos afetados por decisões algorítmicas contestem resultados, garantindo transparência, accountability e mitigando riscos de discriminação inadvertida.

Conforme mencionado por Braga (2019), a inovação tecnológica deve possuir dois componentes: (1) seu desenvolvimento, implantação e uso devem respeitar os direitos e regulamentos aplicáveis, bem como princípios e valores fundamentais, assegurando um "propósito ético", e (2) deve ser tecnicamente robusta e confiável visto que, mesmo com boas intenções ou propósitos, a falta de domínio tecnológico pode gerar danos não intencionais.

Portanto, a construção de sistemas de IA éticos e responsáveis requer a integração de princípios de transparência e responsabilidade, assegurando que a tecnologia sirva ao bem comum e respeite os direitos fundamentais dos indivíduos. Além disso, é imprescindível que esses sistemas sejam acompanhados por mecanismos de supervisão humana e enquadrados em normas jurídicas claras, garantindo que decisões automatizadas possam ser monitoradas, avaliadas e corrigidas quando necessário.

SEGURANÇA DA INFORMAÇÃO

O armazenamento e o tratamento de dados em larga escala tornam as bases de informação potenciais alvos de ataques cibernéticos. Esse cenário evidencia a necessidade de medidas robustas de proteção, envolvendo tanto ferramentas técnicas quanto práticas de governança. Conforme dispõe Oliveira (2025), segurança da informação deixou de ser apenas uma responsabilidade técnica ou departamental e passou a integrar o núcleo estratégico da governança.

Ainda cabe mencionar que a LGPD impõe o dever de adoção de medidas de segurança capazes de mitigar riscos, de modo a assegurar a integridade, a confidencialidade e a disponibilidade das informações. A segurança da informação, portanto, é um elemento central para a construção da confiança no ambiente digital.

CONFLITO COM DIREITOS FUNDAMENTAIS

O monitoramento em larga escala, quando utilizado sem critérios claros e mecanismos de controle, pode ameaçar tanto os direitos fundamentais assegurados pela Constituição Federal, como a privacidade, a igualdade e o devido processo legal. O risco da vigilância indiscriminada revela que a proteção de dados não deve ser tratada apenas como um tema técnico, mas como um aspecto diretamente relacionado à proteção da democracia e à efetividade das garantias constitucionais.

Como assinalado por Cometti (2025), a crescente capacidade de monitorar e analisar comportamentos humanos em larga escala levanta questões significativas sobre direitos fundamentais, privacidade e regulamentação, um alerta que reforça a urgência de normativas que articulem tecnologia, ética e justiça.

Diante disso, é necessário reconhecer que a regulação das tecnologias de monitoramento deve ir além de preocupações meramente operacionais, assumindo caráter normativo e constitucional. Somente a partir da definição de limites claros e da implementação de salvaguardas jurídicas adequadas será possível compatibilizar o avanço tecnológico com a preservação das liberdades individuais e a consolidação do Estado Democrático de Direito.

O avanço do Big Data e da Inteligência Artificial traz benefícios relevantes, mas também desafios que afetam diretamente direitos fundamentais, como privacidade, igualdade e segurança. Assim,

a proteção de dados, a transparência dos algoritmos e a adoção de medidas eficazes de segurança tornam-se exigências essenciais para evitar abusos e garantir confiança no ambiente digital, ficando evidente que o desenvolvimento tecnológico precisa ser acompanhado de responsabilidade, ética e regulações claras, para que a inovação ocorra sem comprometer direitos e princípios fundamentais do Estado Democrático de Direito.

PROJEÇÕES FUTURAS

Conforme delineado, a era digital trouxe consigo um volume sem precedentes de dados, fenômeno que passou a ser denominado Big Data. Esse processo envolve não apenas a coleta massiva de informações, mas também sua análise e processamento em escala inédita. No campo jurídico, o Big Data representa tanto uma promessa de maior eficiência e previsibilidade quanto um risco para a proteção da privacidade e a preservação dos direitos fundamentais.

Segundo Souza (2024), o debate ético sobre o uso de Big Data encontra-se no centro das discussões contemporâneas, especialmente no que diz respeito à privacidade, à dignidade humana e à responsabilidade das instituições. Entretanto, é preciso avançar além das discussões atuais e projetar como o Direito será impactado nas próximas décadas.

Neste contexto, surge a seguinte questão-problema: quais as projeções futuras para o uso do Big Data no Direito, considerando aspectos éticos, regulatórios e sociais. De acordo com Sagiroglu e Sinanc (2013), o Big Data caracteriza-se pelos Vs: volume, variedade, velocidade e veracidade, aos quais autores posteriores acrescentaram o valor. No contexto jurídico, essas características se traduzem em desafios para tribunais, órgãos de controle e advogados, que

passam a lidar com informações cada vez mais dinâmicas, complexas e difíceis de auditar.

Souza (2024) aponta que a coleta e o processamento de dados são tão eficazes que as abordagens tradicionais de proteção da privacidade se mostram inadequadas. A reidentificação de dados anonimizados e a vigilância contínua são exemplos de problemas que deverão se intensificar no futuro.

IMPACTOS JÁ IDENTIFICADOS NO DIREITO

Quanto à privacidade e proteção de dados, o Regulamento Europeu de Proteção de Dados (GDPR) e a Lei Geral de Proteção de Dados brasileira (LGPD) representam marcos normativos que já impactam a prática jurídica. Ambos estabelecem limites claros ao tratamento de dados pessoais e introduzem conceitos como consentimento informado, direito ao esquecimento e *privacy by design*.

Contudo, a implementação ainda enfrenta desafios práticos, como a assimetria de poder entre grandes corporações e indivíduos e a dificuldade de garantir que o consentimento seja realmente livre e informado. No que se refere às questões éticas emergentes, o uso de Big Data já levanta preocupações relacionadas à discriminação algorítmica e à falta de transparência em sistemas de inteligência artificial. Souza (2024) ressalta que a privacidade deve ser entendida não apenas como proteção de dados, mas também como garantia da autonomia e dignidade humana.

Desse modo, observa-se que, embora a GDPR e a LGPD tenham estabelecido bases sólidas para a proteção de dados e para a promoção de práticas mais responsáveis no uso de informações pessoais, a realidade jurídica ainda enfrenta obstáculos relevantes e, nesta seara, a persistência de desequilíbrios entre usuários e grandes organizações, aliada aos riscos de discriminação e opacidade

nos sistemas algorítmicos, evidencia que a proteção da privacidade vai além do cumprimento formal da lei: envolve assegurar condições reais de autonomia, dignidade e controle informacional.

Assim, os impactos já visíveis na área jurídica demonstram a necessidade contínua de aprimoramento regulatório e de mecanismos que tornem efetivos os princípios éticos e jurídicos que orientam a sociedade digital. Ainda, é fundamental garantir a participação ativa da sociedade civil e a implementação de processos de fiscalização transparentes, assegurando que as normas e diretrizes sejam efetivamente cumpridas e adaptadas às novas realidades tecnológicas.

PROJEÇÕES FUTURAS DO BIG DATA NO DIREITO

No tocante à justiça preditiva e jurimetria, no futuro próximo tribunais deverão utilizar algoritmos para analisar padrões jurisprudenciais e sugerir decisões. O Supremo Tribunal Federal já utiliza a IA Victor para classificar recursos, e outros tribunais desenvolvem ferramentas semelhantes. A tendência é que o uso da jurimetria evolua para a decisão judicial preditiva, o que suscitará debates sobre imparcialidade, vieses e legitimidade democrática.

Já no que se refere à regulação global e soberania digital, projeta-se o fortalecimento de um Direito Internacional Digital, com organismos multilaterais promovendo a harmonização de normas. A União Europeia lidera esse processo, mas países como China e EUA disputam o protagonismo regulatório. No futuro, o conceito de soberania digital poderá implicar restrições a fluxos de dados entre nações e exigências de armazenamento local.

Ressalte-se que as projeções para o futuro indicam uma ampliação significativa da responsabilidade jurídica decorrente do uso do Big Data, com reflexos nas esferas civil, penal e administrativa. Tende a consolidar-se a responsabilização de empresas e

organizações por danos causados por decisões automatizadas que resultem em discriminação, exclusão social ou prejuízos concretos aos indivíduos. Isso abrange, por exemplo, a negativa de crédito baseada em algoritmos enviesados ou a utilização de perfis comportamentais que reforcem estigmas sociais.

O debate caminha para o reconhecimento de um dever de diligência tecnológica, impondo às corporações a obrigação de auditar, corrigir e justificar os modelos algorítmicos que utilizam. Novas figuras típicas deverão surgir para lidar com condutas relacionadas à manipulação massiva de dados, disseminação de *deepfakes*, práticas de vigilância abusiva e perfis discriminatórios intencionais. O Direito Penal será chamado a atuar especialmente em situações que envolvam a fraude digital em larga escala, a manipulação informacional de processos eleitorais e a violação dolosa da integridade dos sistemas de dados. Discute-se, nesse contexto, a criação de um Direito Penal da Informação, adaptado à complexidade dos crimes algorítmicos.

Órgãos reguladores, como a Autoridade Nacional de Proteção de Dados (ANPD) no Brasil, deverão assumir papel cada vez mais ativo na fiscalização preventiva e repressiva do uso de dados pessoais. O futuro aponta para um modelo regulatório mais robusto, com poderes ampliados de investigação, imposição de sanções severas e exigência de relatórios de impacto algorítmico. Isso reforça a tendência de fortalecimento do chamado Direito Administrativo Sancionador Digital, voltado à tutela da privacidade, da transparência e da segurança informacional.

Em síntese, a expansão da responsabilidade jurídica no contexto do Big Data exigirá não apenas novas categorias normativas, mas também uma mudança cultural, em que empresas, instituições e indivíduos reconheçam a centralidade da ética da informação e da *accountability* digital como fundamentos de um ordenamento jurídico voltado para a era dos algoritmos.

INTEGRAÇÃO COM *BLOCKCHAIN* E IDENTIDADES DIGITAIS. DIREITO AMBIENTAL E MONITORAMENTO DIGITAL

O futuro aponta para a consolidação das identidades digitais soberanas (*Self-Sovereign Identity* – SSI), em que indivíduos terão maior controle sobre seus dados, armazenando-os em redes *blockchain* descentralizadas. Essa inovação poderá redefinir conceitos jurídicos ligados à personalidade, à propriedade e ao consentimento informado.

Na área socioambiental, especialmente no contexto amazônico, o uso de Big Data permitirá fiscalização em tempo real de queimadas, desmatamento e pesca predatória. Isso ampliará a eficiência da tutela ambiental, mas exigirá adaptações no Direito Ambiental e Agrário, com maior uso de provas digitais e relatórios automatizados em processos administrativos e judiciais.

Assim, denota-se que a adoção de identidades digitais baseadas em blockchain e o uso crescente de Big Data para monitoramento ambiental anunciam mudanças significativas para o campo jurídico. Essas tecnologias podem tanto ampliar o controle dos indivíduos sobre suas próprias informações quanto tornar mais ágil e precisa a fiscalização de práticas lesivas ao meio ambiente.

Entretanto, tais avanços exigem ajustes nas estruturas normativas e nos métodos de produção de provas, de modo a garantir segurança jurídica, respeito aos direitos fundamentais e efetividade na proteção ambiental em um contexto marcado pela digitalização e pela automação.

DESAFIOS ÉTICOS E FILOSÓFICOS

As projeções futuras não podem ser dissociadas de uma reflexão ética. Conforme Floridi (2014), é necessário adotar uma ética da informação, que coloque o indivíduo no centro da governança digital.

Sob uma perspectiva foucaultiana, o Big Data pode ser visto como um novo dispositivo de poder-saber, no qual a vigilância se torna difusa e permanente. A tarefa do Direito será equilibrar inovação e liberdade, evitando a consolidação de uma sociedade de vigilância total.

As projeções futuras do Big Data no Direito apontam para um campo de grandes oportunidades e graves riscos. De um lado, há a promessa de maior eficiência, transparência e previsibilidade; de outro, a ameaça de vigilância constante, discriminação algorítmica e erosão de direitos fundamentais. O futuro do Big Data no Direito dependerá da capacidade de articulação entre regulação, ética e inovação tecnológica.

A construção de um ecossistema digital justo exige não apenas leis eficazes, como o GDPR e a LGPD, mas também uma cultura jurídica que valorize a dignidade humana diante da lógica dos algoritmos. Isso requer, ainda, a capacitação contínua de profissionais do Direito e de tecnologia, promovendo uma compreensão ética e crítica do impacto das decisões automatizadas sobre a sociedade.

CONSIDERAÇÕES FINAIS: RUMO A UM DIREITO DIGITAL RESPONSÁVEL E HUMANOCÊNTRICO

A era do Big Data e da Inteligência Artificial impõe ao Direito uma reconfiguração profunda e urgente. Os desafios à discriminação, privacidade, transparência, poder e vigilância exigem um novo contrato social para a era digital. A insuficiência das abordagens jurídicas tradicionais demanda uma resposta multifacetada, combinando legislações robustas, interpretações inovadoras dos direitos fundamentais, supervisão eficaz e mecanismos de controle judicial (Hoffmann-Riem, 2020).

O desenvolvimento do Big Data e da IA inaugura uma fase inédita na sociedade da informação, caracterizada pela ampla captação, tratamento e utilização estratégica de dados em larga escala, sendo indubitável que esse fenômeno abre caminhos promissores para o crescimento econômico, para a modernização da gestão pública e para o fomento da inovação tecnológica.

Entretanto, também levanta questões jurídicas relevantes, exigindo do ordenamento nacional respostas adequadas para assegurar a privacidade, a transparência nas práticas de tratamento e a efetividade dos direitos fundamentais. Ainda, impõe a necessidade de *frameworks* éticos que orientem a utilização desses dados, garantindo que a inovação tecnológica esteja alinhada aos princípios de justiça e proteção dos cidadãos.

Conforme preceituam Orsini e Lara:

> [...] infere-se que a assunção pelo universo jurídico das análises oriundas de processos de big data tem potencial para a geração de uma nova onda de acesso material à justiça. Isto será possível por meio do ganho de eficiência proporcionado pela lógica algoritmal empregada em grande escala e pela ação conjunta dos atores oficiais que possuem a missão institucional de dar respostas aos conflitos sociais. Uma grande janela de oportunidades para a adoção maciça do big data surge no Brasil com a expansão do processo judicial eletrônico e o alargamento da base de dados computacionais sobre a litigiosidade. **Tal ganho, contudo, alerta para o risco de violações da intimidade e da vida privada**, quer pelas empresas, quer pelo Estado, a partir dos rastros eletrônicos deixados pelas próprias interações sociais. **A discussão sobre os limites desta apropriação ganha novos contornos na temática do controle social e a criação de novos instrumentos de proteção se mostra necessária**. Uma nova onda de acesso material à justiça fundamentada no big data deverá necessariamente obedecer alguns pressupostos, principalmente no que tange ao controle popular sobre a criação dos algoritmos computacionais.

> Novos desenhos institucionais deverão ser criados com o reconhecimento de grupos sociais e suas bandeiras históricas de luta, de modo a conferir legitimidade social para as conquistas tecnológicas significativas do século XXI (Orsini; Lara, 2017, p. 89, grifos nossos)

Nesse cenário, a Lei Geral de Proteção de Dados (LGPD) surge como um marco regulatório de suma importância, ao buscar harmonizar os avanços tecnológicos com a segurança jurídica, garantindo aos cidadãos proteção contra abusos e incentivando o uso ético e responsável das informações.

Segundo Rank e Berberi (2022), em que pese a importância do Big Data e da IA, no que concerne à utilização de dados pessoais há uma grande obscuridade no ambiente digital, pouco se tendo conhecimento das implicações possíveis na captação, no armazenamento, no tratamento dos dados pessoais dos indivíduos quando lançados em redes digitais, sendo certo que a má utilização de dados pessoais pode afetar não somente o direito fundamental à privacidade, mas também o sistema de direito fundamental como um todo.

No mais, o dinamismo das transformações digitais impõe aos profissionais do Direito a necessidade de constante atualização, e ao Estado a tarefa de aprimorar suas instituições, sob pena de se tornar defasado diante das novas formas de manipulação de dados. Para Cathy O'neil (2021), temos que explicitamente embutir melhores valores em nossos algoritmos, criando modelos de Big Data que seguem nossa conduta ética, sendo que o desafio para os cientistas de dados é entender os ecossistemas para os quais estão avançando e apresentar não apenas os problemas, mas também as possíveis soluções.

Nesta conjectura, a análise desenvolvida ao longo deste estudo permite observar que o Big Data e a Inteligência Artificial não são apenas instrumentos tecnológicos, mas fatores que impactam de forma profunda o ordenamento jurídico, os direitos fundamentais e a

governança digital. O estudo evidencia que, embora existam marcos regulatórios como a LGPD e o Marco Civil da Internet, o Direito tradicional enfrenta dificuldades em lidar com decisões automatizadas, discriminação algorítmica e coleta massiva de dados. As práticas de Big Data frequentemente extrapolam os limites previstos, revelando lacunas de proteção à privacidade, insuficiência de mecanismos de accountability e desafios para a fiscalização estatal e corporativa. Esse resultado reforça a necessidade de adaptação normativa e criação de instrumentos jurídicos mais sofisticados e flexíveis, capazes de lidar com a complexidade e a velocidade das tecnologias digitais.

Outro aspecto relevante refere-se à promoção de uma visão humanocêntrica do Direito Digital. A pesquisa identifica que a integração de princípios de ética, transparência e proteção de dados nos sistemas de IA e Big Data não é apenas desejável, mas essencial para assegurar a dignidade humana, prevenir discriminação e garantir o exercício pleno da cidadania. A análise de casos envolvendo vigilância estatal, publicidade direcionada e algoritmos de triagem evidencia a necessidade de implementação de políticas públicas e mecanismos regulatórios que promovam o uso responsável, seguro e transparente dos dados. Dessa forma, o estudo oferece subsídios concretos para a formulação de normas, diretrizes e estratégias que harmonizem inovação tecnológica com direitos fundamentais.

Em síntese, os resultados da pesquisa confirmam que o avanço do Big Data representa tanto oportunidades quanto riscos. As conclusões indicam que o ordenamento jurídico brasileiro, ao integrar princípios éticos, normas claras e mecanismos de fiscalização eficientes, pode transformar os desafios identificados em oportunidades para consolidar um Direito Digital robusto, responsável e alinhado aos valores constitucionais. Dessa forma, o estudo alcança seu objetivo de analisar criticamente os impactos jurídicos do Big Data e da Inteligência Artificial, evidenciando tanto suas potencialidades quanto os desafios regulatórios e éticos que se impõem ao ordenamento jurídico contemporâneo.

Assim, conclui-se que o Big Data e sua ampla utilização pela inteligência Artificial representam, ao mesmo tempo, um desafio e uma oportunidade para o ordenamento jurídico nacional: o desafio de acompanhar e regular práticas em contínua evolução e a oportunidade de consolidar a proteção de direitos fundamentais, o fortalecimento da democracia e a construção de uma relação de confiança entre sociedade e tecnologia na era digital.

O êxito jurídico na era do Big Data/IA dependerá do equilíbrio entre inovação e responsabilidade, para o bem da sociedade. A tarefa do Direito não é frear a inovação, mas moldá-la para que sirva ao bem-estar individual e coletivo, reafirmando os valores constitucionais de igualdade e dignidade em um mundo cada vez mais mediado por algoritmos. O jurista, encontrando na Constituição um porto seguro, deve ser protagonista na construção de uma sociedade digital mais equitativa, transparente e humanocêntrica (Azevedo; Jahn, 2020). Isso implica uma responsabilidade contínua do Direito em garantir que o poder transformador do Big Data e da IA seja direcionado para o benefício da humanidade, alinhado aos princípios éticos e aos direitos fundamentais e não para a sua subserviência.

REFERÊNCIAS

AZEVEDO, André Jobim de; JAHN, Vitor Kaiser. **Direito do Trabalho e Novas Tecnologias**: Inteligência Artificial, Big Data e Discriminação Pré-contratual. Documento fornecido, 2020.

BASSO, Douglas Eduardo. **Big Data.** Curitiba, PR: Contentus, 2020. E-book. Disponível em: https://plataforma.bvirtual.com.br. Acesso em: 17 ago. 2025.

BRAGA, Carolina Henrique da Costa. **Decisões automatizadas e discriminação**: pesquisa de propostas éticas e regulatórias no policiamento preditivo. 2019. Dissertação (Mestrado) – Estácio, Rio de Janeiro, 2019. Disponível em: https://dissertacoes-estacio.s3.amazonaws.com/direito/2019/4679621_carolina-henrique-da-costa-braga.pdf. Acesso em: 23 ago. 2025.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 26 ago. 2025.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Lei Geral de Proteção de Dados Pessoais – LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 22 ago. 2025.

COMETTI, Marcelo Tadeu. **Vigilância Algorítmica e Direito**: Desafios e Regulação. 2025. Disponível em: https://legale.com.br/blog/vigilancia-algoritmica-desafios-e-regulamentacao-juridica/. Acesso em: 23 ago. 2025.

FLOREA, Diana; FLOREA, Silvia. **Big Data e as implicações éticas da privacidade de dados na pesquisa do ensino superior.** 2020. Disponível em: https://doi.org/10.3390/su12208744. Acesso em: 22 ago. 2025.

FLORIDI, L. **A quarta revolução**: como a infosfera está remodelando a realidade humana. Oxford: Oxford University Press, 2014.

HOFFMANN-RIEM, Wolfgang. Big Data e Inteligência Artificial: Desafios para o Direito. **Revista Estudos Institucionais**, v. 6, n. 2, p. 431-506, mai./ago. 2020.

MUSETI, C.; FINOTO, L. **O Big Data e a Lei Geral de Proteção de Dados**. 1. ed. São Paulo, SP: Bookwire - Editora Dialética, 2023. Disponível em: https://elibro.net/pt/ereader/univem/236580?page=24. Acesso em: 17 ago. 2025.

OLIVEIRA, Alessandro Virgini de. Segurança da informação e a proteção de dados. *In*: AURUM EDITORA. **Integração Multidisciplinar no Conhecimento**. Curitiba: Aurum, 2025. Disponível em: https://aurumpublicacoes.com/index.php/editora/article/view/73/64. Acesso em: 23 ago. 2025.

O'NEIL, Cathy. **Algoritmos de Destruição em Massa**: Como o Big Data Aumenta a Desigualdade e Ameaça a Democracia. Tradução de Rafael Abraham. São Paulo, SP: Editora Rua do Sabão, 2021.

ORSINI, Adriana Goulart de Sena; LARA, Caio Augusto Souza. **O fenômeno do Big Data e os pressupostos para uma nova onda de acesso material à justiça.** Publicações Científicas e Culturais, Repositório Institucional da UFMG, 2017.

PUGLIESI, Márcio; BRANDÃO, André Martins. Uma Conjectura Sobre as Tecnologias de Big Data na Prática Jurídica. **Revista da Faculdade de Direito da UFMG**, Belo Horizonte, n. 67, p. 453-482, jul./dez. 2015.

RANK, Angela Teresinha; BERBERI, Marco Antônio Lima. Big Data e direitos fundamentais sob o enfoque da Lei Geral de Proteção de Dados (LGPD). **International Journal of Digital Law**, Belo Horizonte, ano 3, n. 2, p. 9-28, mai./ago. 2022.

SAGIROGLU, S.; SINANC, D. **Big Data**: uma revisão. Conferência Internacional sobre Tecnologias e Sistemas de Colaboração (CTS 2013), San Diego, 2013. p. 42–47.

SOUZA, Jussara Feitosa de. Privacidade e dados pessoais: o debate ético sobre o uso de Big Data. **Revista Ilustração**, Cruz Alta, v. 5, n. 6, p. 27-51, 2024.

Jardson Ferreira da Silva

Advogado e Mestrando em Direito Digital no Centro Universitário Eurípedes de Marília – UNIVEM – Marília/SP, Brasil.

E-mail: jardsonsilva@hotmail.com

Mara Augusto Dias

Procuradora-Geral e Mestranda em Direito Digital no Centro Universitário Eurípedes de Marília – UNIVEM – Marília/SP, Brasil.

E-mail: mara_augusto@hotmail.com

Mirella Fernandes Atanázio

Advogada e Mestranda em Direito Digital no Centro Universitário Eurípedes de Marília (UNIVEM).

E-mail: mirella.atanazio97@gmail.com

Rodrigo Murad Vitoriano

Procurador Jurídico e Mestrando em Direito Digital no Centro Universitário Eurípedes de Marília – UNIVEM – Marília/SP, Brasil.

E-mail: adv.rmv@hotmail.com