



CURSO DE DIREITO

GABRIEL LIMA RANGEL

**INTELIGÊNCIA ARTIFICIAL, AUTOMAÇÃO E RELAÇÕES DE
TRABALHO: DESAFIOS JURÍDICOS NO CENÁRIO
CONTEMPORÂNEO**

**MONTENEGRO
2026**

GABRIEL LIMA RANGEL

**INTELIGÊNCIA ARTIFICIAL, AUTOMAÇÃO E RELAÇÕES DE TRABALHO:
DESAFIOS JURÍDICOS NO CENÁRIO CONTEMPORÂNEO**

Trabalho de Conclusão apresentado ao
Curso da Universidade de Santa Cruz do
Sul, UNISC, para obtenção do título de
Bacharel em Direito.

Orientadora: Profa. Dra. Suzéte da Silva Reis

**MONTENEGRO
2026**

AGRADECIMENTOS

Dedico este Trabalho de Conclusão de Curso, em especial, à minha mãe, que não está mais presente entre nós, mas que sempre será minha maior inspiração. Seu amor, seus ensinamentos, sua força e seus valores permanecem vivos em minha memória e em cada conquista alcançada ao longo da minha vida. Mesmo em sua ausência, sinto que sua presença continua me guiando e me dando forças para seguir em frente e nunca desistir dos meus sonhos.

Dedico também este trabalho aos meus colegas, professores e amigos, que fizeram parte dessa importante caminhada acadêmica, compartilhando conhecimentos, desafios e aprendizados ao longo dessa trajetória. Cada momento vivido durante a graduação contribuiu de forma significativa para minha formação pessoal e profissional.

Que esta conquista represente não apenas o encerramento de um ciclo, mas também o início de novos caminhos, oportunidades e desafios na busca constante pelo conhecimento e pela realização dos meus objetivos.

“Sem amor não poderíamos sobreviver. Os seres humanos são criaturas sociais, e sentir-se valorizados uns pelos outros é a própria base da vida em comunidade.”

Dalai Lama

RESUMO

O presente trabalho analisa criticamente os impactos da inteligência artificial (IA) e da automação nas relações de trabalho contemporâneas, especialmente no contexto brasileiro, destacando os desafios jurídicos emergentes. Inseridos na Quarta Revolução Industrial, sistemas algorítmicos e plataformas digitais reconfiguram o vínculo empregatício tradicional, intensificando a subordinação algorítmica, a precarização e a vigilância constante sobre os trabalhadores. A pesquisa evidencia que a Consolidação das Leis do Trabalho (CLT) e o arcabouço normativo vigente mostram-se insuficientes para enfrentar as novas realidades laborais mediadas por IA. São analisados os riscos da discriminação algorítmica, da violação de direitos fundamentais como a privacidade, a igualdade e a proteção de dados, bem como os limites de responsabilização civil e penal em face das condutas autônomas de sistemas inteligentes. Com base em experiências internacionais, como o AI Act da União Europeia, propõem-se diretrizes normativas urgentes: transparência algorítmica, responsabilização objetiva dos empregadores, direito à revisão humana de decisões automatizadas, auditoria independente dos sistemas de IA e fortalecimento da proteção de dados trabalhistas. O estudo conclui que o direito do trabalho brasileiro necessita de uma reinvenção normativa disruptiva e célere, sob pena de obsolescência frente à consolidação do domínio algorítmico e da servidão digital no mercado de trabalho.

Palavras-chave: Automação; Inteligência Artificial; Proteção De Dados; Responsabilidade Civil; Subordinação Algorítmica.

ABSTRACT

This study critically examines the impacts of artificial intelligence (AI) and automation on contemporary labor relations, with particular emphasis on the Brazilian context, highlighting emerging legal challenges. Embedded within the Fourth Industrial Revolution, algorithmic systems and digital platforms are reshaping traditional employment bonds, intensifying algorithmic subordination, precariousness, and constant worker surveillance. The research demonstrates that the Brazilian Consolidation of Labor Laws (CLT) and the current legal framework are insufficient to address labor realities mediated by AI. It analyzes the risks of algorithmic discrimination, violations of fundamental rights such as privacy, equality, and data protection, as well as the limits of civil and criminal liability concerning autonomous conduct by intelligent systems. Based on international experiences such as the European Union's AI Act, urgent normative guidelines are proposed: algorithmic transparency, strict employer liability, the right to human review of automated decisions, independent AI system audits, and the strengthening of labor data protection. The study concludes that Brazilian labor law requires a disruptive and prompt normative reinvention, or it risks becoming obsolete in the face of algorithmic dominance and digital servitude in the labor market.

Keywords: Artificial Intelligence. Labor Law. Automation. Algorithmic Subordination. Data Protection. Civil Liability.

SUMÁRIO

INTRODUÇÃO.....	8
2. AUTOMAÇÃO E INTELIGÊNCIA ARTIFICIAL: CONTEXTO E CONCEITOS	12
2.1. Impactos da IA nas Relações de Trabalho.....	13
2.2. Discriminação Algorítmica e Novos Desafios Jurídicos	14
2.3. Proteção de Dados e Direitos Fundamentais	15
2.4. Responsabilidade Civil por Danos Causados por Sistemas de Inteligência Artificial nas Relações de Trabalho	15
2.5. Transparência Algorítmica, Explicabilidade e o Direito de Contestação nas Decisões Automatizadas.....	19
3. ALGORITMOS, CONTROLE SOCIAL E CAPITALISMO DE VIGILÂNCIA	22
3.1. Inteligência artificial e controle social: análise de exemplos.....	24
3.2. Dos direitos fundamentais e novas tecnologias	28
3.3. Consequências do uso de IA para controle social	30
3.4. Desafios Regulatórios e Perspectivas Jurídicas para o Uso da Inteligência Artificial	33
4. DECISÕES AUTOMATIZADAS E LIMITES DA CLT	41
4.1. Jurisprudência, Legislação e Tendências Regulatórias	41
4.2. Propostas de Atualização Normativa.....	45
4.3. <i>A Quarta Revolução Industrial e o Novo Paradigma do Trabalho</i>	46
4.4. Desafios jurídicos na proteção dos direitos fundamentais do trabalhador.....	47
4.5. Futuro da legislação trabalhista: tendências e propostas	50
4.6. Perspectivas Futuras e a Necessidade de Regulação Jurídica da Inteligência Artificial no Brasil.....	53
CONCLUSÃO.....	57
REFERÊNCIAS	59

INTRODUÇÃO

O avanço da inteligência artificial (IA) e da automação vem redefinindo o mercado de trabalho global, desencadeando transformações profundas e irreversíveis nas relações laborais. Em um cenário marcado pela chamada Quarta Revolução Industrial, tecnologias digitais, algoritmos e robôs passaram a desempenhar funções tradicionalmente reservadas ao trabalho humano, alterando a dinâmica produtiva e impondo novos desafios à ordem jurídica. A consolidação do capitalismo de dados, a implementação massiva de sistemas de decisão automatizada e o surgimento de plataformas digitais de trabalho desafiam a legislação trabalhista clássica, fundada sobre bases do século XX e incapaz de oferecer respostas à complexidade do novo contexto. O desafio central consiste em compatibilizar inovação e eficiência com a preservação dos direitos fundamentais dos trabalhadores, enfrentando riscos como a precarização, a discriminação algorítmica e a intensificação do controle sobre a força de trabalho.

O presente trabalho mergulha na análise crítica dos impactos provocados pela IA e pela automação sobre as relações normativas e a proteção do trabalhador no Brasil. O objetivo é evidenciar lacunas e contradições do arcabouço legal diante das novas formas de organização do trabalho, explorando a necessidade de revisão profunda dos institutos tradicionais. A abordagem parte da constatação de que o modelo vigente — baseado em vínculo formal, subordinação clássica e proteção rígida — está sendo progressivamente esvaziado por estruturas descentralizadas e baseadas em dados, que desafiam os conceitos de emprego, jornada e remuneração. A centralidade dos algoritmos nos processos de recrutamento, gestão e demissão amplia o potencial discriminatório e cria novas formas de subordinação, muitas vezes invisíveis ao direito atual.

Sob esse prisma, a pesquisa propõe não apenas diagnosticar as consequências do uso intensivo de IA e automação, mas também apontar diretrizes para a construção de um direito do trabalho compatível com o futuro digital. Serão analisadas experiências nacionais e internacionais, bem como

propostas legislativas em debate, com destaque para temas como explicabilidade algorítmica, transparência, proteção de dados pessoais e atualização dos direitos sociais. O enfrentamento dos riscos de exclusão e precarização exige visão estratégica e ação legislativa proativa, sob pena de condenar milhões de trabalhadores à marginalização digital. A disseminação de sistemas baseados em inteligência artificial e automação nas relações laborais contemporâneas impõe ao direito do trabalho um desafio sem precedentes: garantir a proteção dos direitos fundamentais do trabalhador em um ambiente dominado por decisões automatizadas, controle algorítmico e flexibilização dos vínculos tradicionais. A legislação brasileira, ainda ancorada nos paradigmas da CLT e nas premissas do emprego formal, demonstra crescente incapacidade de responder a fenômenos como a subordinação algorítmica, o uso discriminatório de dados e a diluição da responsabilidade empregatícia nas plataformas digitais. Neste contexto, impõe-se a indagação central: Como o direito do trabalho brasileiro pode ser atualizado para assegurar a proteção efetiva dos trabalhadores diante do avanço irreversível da inteligência artificial e da automação, especialmente no que tange à prevenção de discriminações, à garantia do acesso isonômico ao emprego e à preservação da dignidade humana?

O objetivo analisar criticamente os impactos da inteligência artificial e da automação nas relações normativas e na proteção dos direitos fundamentais do trabalhador no Brasil, identificando desafios e propondo alternativas jurídicas para compatibilizar inovação tecnológica e dignidade do trabalho humano.

O presente trabalho tem como objetivo investigar as transformações impostas pela inteligência artificial e automação ao modelo tradicional de relação de trabalho, com ênfase nas novas formas de subordinação, controle e gestão da força de trabalho que emergem nesse contexto. Além disso, busca-se examinar os riscos concretos de discriminação algorítmica, precarização e exclusão social derivados da implementação de sistemas de decisão automatizada no ambiente laboral. Por fim, propõe-se apresentar diretrizes para a atualização da legislação trabalhista, contemplando a regulamentação da transparência algorítmica, a proteção de dados pessoais e a revisão dos

mecanismos clássicos de proteção do trabalhador, de modo a adequar o direito do trabalho às exigências de uma sociedade profundamente impactada pelo avanço tecnológico.

A escolha do tema se justifica pela urgência do debate sobre os limites e as possibilidades do direito do trabalho em face das rupturas provocadas pela automação e pela inteligência artificial. O mercado de trabalho global enfrenta uma transformação estrutural, em que algoritmos, plataformas digitais e sistemas inteligentes substituem processos humanos, redefinindo a natureza do emprego e das garantias sociais. No Brasil, a legislação permanece atrelada a conceitos do século passado, revelando-se ineficaz diante dos riscos de precarização, intensificação da desigualdade e novas formas de discriminação. O impacto sobre trabalhadores vulneráveis, como mulheres, minorias raciais e pessoas com deficiência, é potencializado pela ausência de mecanismos de controle e de transparência nas decisões automatizadas.

Além disso, a emergência da sociedade do big data e do capitalismo de vigilância impõe ao legislador o dever de revisitar as bases do direito social, incorporando a proteção de dados pessoais e a explicabilidade algorítmica como dimensões fundamentais da dignidade humana no ambiente de trabalho. Estudos recentes do Ministério Público do Trabalho, da Organização Internacional do Trabalho e de centros de pesquisa internacionais alertam para o risco de retrocesso social e esvaziamento dos direitos conquistados, caso não haja uma reação normativa à altura dos desafios. Este trabalho, portanto, se propõe a ocupar a fronteira do debate, fundamentando-se em uma perspectiva crítica e propositiva, para contribuir com a reinvenção do direito do trabalho diante do avanço tecnológico.

A pesquisa adota abordagem qualitativa, de caráter exploratório e crítico, fundamentando-se em revisão bibliográfica, análise documental e estudo de casos emblemáticos. Inicialmente, realiza-se levantamento e exame das principais obras doutrinárias nacionais e estrangeiras sobre automação, inteligência artificial e relações de trabalho, incluindo livros, artigos, relatórios técnicos e documentos institucionais (ex.: Ministério Público do Trabalho, OIT, União Europeia). A literatura selecionada prioriza produções dos últimos dez

anos, com destaque para textos que tratam dos efeitos da IA na estrutura do emprego, discriminação algorítmica, proteção de dados pessoais e desafios jurídicos emergentes.

Complementarmente, a análise documental abrange legislação nacional (CLT, LGPD, Constituição Federal, EC 115/2022), decisões judiciais (TST, TRT), notas técnicas e pareceres de órgãos oficiais. A pesquisa examina, ainda, casos paradigmáticos internacionais (Amazon, Uber, Xsolla) e nacionais, utilizando-os como base para compreender os impactos concretos da automação e IA no ambiente laboral. O método jurídico-dedutivo orienta o desenvolvimento do raciocínio, partindo das normas e princípios aplicáveis para a crítica das práticas e proposição de alternativas normativas. O tratamento dos dados prioriza a triangulação entre doutrina, jurisprudência e casos práticos, garantindo densidade teórica e aplicabilidade dos resultados.

Por fim, para garantir rigor científico e atualização, a pesquisa consulta periódicos indexados, bancos de dados acadêmicos e relatórios de organismos internacionais de referência. O objetivo é construir uma análise robusta, orientada por evidências, capaz de fundamentar propostas inovadoras para a regulação do trabalho na era digital.

2. AUTOMAÇÃO E INTELIGÊNCIA ARTIFICIAL: CONTEXTO E CONCEITOS

O fenômeno da automação produtiva e o surgimento da inteligência artificial constituem marcos da chamada Quarta Revolução Industrial, conceito cunhado por Klaus Schwab para definir o momento em que tecnologias digitais, biotecnologia e sistemas ciber-físicos passaram a integrar todas as dimensões da economia e da sociedade (Schwab, 2016). A inteligência artificial, em particular, consiste em sistemas computacionais capazes de processar, aprender e tomar decisões de forma autônoma, imitando capacidades tradicionalmente humanas como raciocínio, análise, generalização e adaptação (Copeland, 2021). O avanço acelerado dessas tecnologias tem reconfigurado a produção, o consumo e as relações sociais, impulsionando a economia do big data e consolidando o capitalismo de dados.

No contexto do trabalho, a automação se manifesta pela substituição de funções repetitivas, manuais e mesmo intelectuais por máquinas, robôs e softwares inteligentes. Esse processo, longe de ser neutro, traz impactos diretos sobre a distribuição do emprego, a remuneração e o papel do trabalhador na sociedade. O Brasil experimenta, nos últimos anos, a adoção crescente de sistemas de automação e IA nos setores de serviços, indústria e comércio, impulsionando ganhos de produtividade, mas também alimentando o desemprego estrutural e a intensificação da exploração laboral (Antunes, 2018; Durand, 2021).

Na literatura internacional, autores como Zuboff (2020) descrevem o surgimento do capitalismo de vigilância, em que o controle de dados pessoais e a análise comportamental se tornam os motores da acumulação de valor. Já Prassl (2017) e De Stefano (2016) analisam a emergência do trabalho via plataformas digitais, marcadas por vínculos precários, opacidade nas relações de poder e descentralização dos mecanismos clássicos de proteção social. A inteligência artificial, ao mesmo tempo em que cria oportunidades, amplia riscos de precarização, discriminação e invisibilidade jurídica do trabalhador.

2.1. Impactos da IA nas Relações de Trabalho

A introdução massiva de inteligência artificial e automação nas relações de trabalho não é apenas uma tendência, é a nova realidade global. Plataformas digitais, sistemas de recrutamento automatizado, robôs em ambientes industriais e softwares de gestão baseados em algoritmos já ocupam posições estratégicas em empresas de todos os setores. O efeito é disruptivo: funções são extintas, novos postos surgem em áreas de alta qualificação tecnológica, e o conceito clássico de emprego perde sentido diante de modelos flexíveis e vínculos instáveis (Delgado, 2020; Goldschmidt & Cani, 2022). A literatura evidencia que a IA não só substitui tarefas humanas, mas também potencializa a hiperexploração, a vigilância constante e a personalização extrema do controle do trabalhador.

A obra coordenada pelo Ministério Público do Trabalho (2022) demonstra que algoritmos são usados em processos de seleção, avaliação de produtividade e até decisões de desligamento, muitas vezes sem transparência ou possibilidade de contestação. O “controle algorítmico” fragmenta o poder de negociação coletiva, dificulta a organização sindical e cria novas formas de subordinação, conhecidas como “subordinação algorítmica”. Casos documentados internacionalmente e no Brasil apontam para o crescimento de ambientes de trabalho mediados por IA, com aumento da precarização, intensificação de jornadas e adoecimento mental por hiperconectividade e pressão por resultados (MPT, 2022; PRASSL, 2017).

Estudos comparativos mostram que, enquanto setores altamente qualificados têm ganhos salariais e oportunidades, a maioria dos trabalhadores é empurrada para funções intermediadas por plataformas digitais, sem proteção social ou vínculo formal (De Stefano, 2016). A ausência de regulamentação específica para decisões automatizadas e o vácuo normativo sobre a responsabilidade civil dos sistemas de IA agravam o cenário. O trabalho humano passa a ser objeto de análise estatística, previsões preditivas e classificação algorítmica, redefinindo o próprio sentido da dignidade do trabalhador.

2.2. Discriminação Algorítmica e Novos Desafios Jurídicos

O uso de algoritmos em processos seletivos, avaliações de desempenho e demissões está longe de ser neutro. Os chamados “vieses algorítmicos” reproduzem e amplificam discriminações já existentes no mercado de trabalho, como racismo, sexismo e exclusão de pessoas com deficiência. O caso emblemático da Amazon, relatado por Pantoja e Leão (2022), revelou que sistemas de IA podem excluir candidaturas femininas simplesmente porque os bancos de dados históricos foram alimentados por padrões discriminatórios. Estudos de Harvard demonstram que trabalhadores com perfis atípicos ou dados “incomuns” são sistematicamente invisibilizados por sistemas preditivos, mesmo quando mais qualificados (MPT, 2022).

O problema central é a ausência de mecanismos de explicação e contestação das decisões automatizadas. O artigo 20 da LGPD brasileira impõe limites e exige transparência nos processos decisórios automatizados, mas sua efetividade ainda é mínima diante da opacidade dos sistemas usados por grandes empresas (De Trffé & Medon, 2020; Fonseca, 2021). O controle social e jurídico sobre algoritmos é, hoje, o principal desafio regulatório para impedir que a IA perpetue a marginalização de grupos vulneráveis no mercado de trabalho.

Doutrina e jurisprudência internacional vêm exigindo a implementação de práticas de “auditabilidade algorítmica” e “explicabilidade” das decisões, como já previsto em regulamentos da União Europeia e discutido na literatura brasileira (Rapôso et al., 2019; De Andrade & Faccio, 2019). No Brasil, a lentidão da reação legislativa expõe milhões de trabalhadores a riscos de exclusão, sem possibilidade de defesa frente a decisões tomadas por sistemas opacos e inacessíveis.

2.3. Proteção de Dados e Direitos Fundamentais

A regulação da proteção de dados é o novo front dos direitos fundamentais no trabalho. A inclusão da proteção de dados pessoais no artigo 5º da Constituição Federal, por meio da Emenda Constitucional 115/2022, reflete a centralidade do tema no século XXI. A LGPD, em vigor desde 2020, estabelece princípios como finalidade, necessidade, transparência, não discriminação e responsabilização; todos violados quando sistemas de IA operam sem controles efetivos (Pinheiro, 2020).

No ambiente laboral, a coleta e o tratamento massivo de dados, inclusive sensíveis, aumentam o potencial de monitoramento abusivo, avaliação discriminatória e manipulação de comportamentos. Jurisprudência do TST e orientações do Ministério Público do Trabalho alertam para o risco de violação à intimidade, à privacidade e à autodeterminação informativa de trabalhadores submetidos à vigilância digital permanente (Brasil, 2023). O problema é agravado pela adoção de mecanismos de scoring, classificação de produtividade e análise preditiva de desempenho, quase sempre sem consentimento válido e transparente.

A doutrina defende que a regulação eficaz da IA no trabalho exige a convergência entre o direito do trabalho, a proteção de dados e o direito antidiscriminatório, sob pena de retrocesso social. A ausência de accountability e de regras claras de compartilhamento de dados entre empregadores, plataformas e agentes públicos ameaça a integridade do sistema de proteção trabalhista (De Teffé & Viola, 2020).

2.4. Responsabilidade Civil por Danos Causados por Sistemas de Inteligência Artificial nas Relações de Trabalho

A expansão da inteligência artificial nas relações de trabalho trouxe consigo não apenas ganhos de produtividade e automação, mas também uma série de questionamentos jurídicos acerca dos danos eventualmente produzidos

por decisões automatizadas. Quando algoritmos passam a interferir diretamente em admissões, promoções, avaliações de desempenho, desligamentos e monitoramento constante da produtividade, o debate jurídico deixa de se concentrar apenas na inovação tecnológica e passa a enfrentar uma questão essencial: quem responde quando a tecnologia causa prejuízo ao trabalhador. Não se trata de hipótese abstrata, mas de realidade concreta, pois a automação decisória já afeta direitos patrimoniais, morais, psicológicos e existenciais no ambiente laboral, exigindo do Direito respostas compatíveis com a nova estrutura tecnológica de poder (Bittar, 2005).

A responsabilidade civil brasileira foi tradicionalmente construída sobre a ideia de ato ilícito praticado por uma pessoa, exigindo a presença de dano, nexo causal e imputação jurídica para fins reparatórios. Entretanto, a introdução de sistemas algorítmicos complexos alterou significativamente essa lógica, uma vez que determinadas decisões passam a ser tomadas por mecanismos automatizados que operam mediante cruzamento de dados, padrões estatísticos e inferências preditivas, muitas vezes sem interferência humana imediata. Essa circunstância gera dificuldade na identificação direta da origem do dano, especialmente quando o prejuízo decorre de uma cadeia tecnológica composta por desenvolvedores, bancos de dados, plataformas, programações internas e decisões empresariais automatizadas. Nesse sentido, observa-se que a complexidade técnica da inteligência artificial não elimina a responsabilidade jurídica, pois a inovação tecnológica não pode servir como instrumento de evasão do dever de reparar lesões produzidas no exercício da atividade econômica.

Nesse ponto, é pertinente destacar o entendimento doutrinário acerca da necessidade de repensar os critérios tradicionais de imputação diante da autonomia crescente dos sistemas inteligentes. Como advertiu Good ao refletir sobre o avanço das máquinas autônomas:

[...]Deixe que uma máquina ultra-inteligente seja definida como uma máquina que pode ultrapassar de longe todas as atividades intelectuais de qualquer homem, por mais inteligente que seja. Uma vez que a concepção de máquinas é uma destas atividades intelectuais, uma máquina ultra-inteligente poderia conceber máquinas ainda melhores; haveria então inquestionavelmente uma 'explosão de inteligência', e a

inteligência do homem seria deixada muito para trás. Assim, a primeira máquina ultra-inteligente é a última invenção que o homem precisa fazer, desde que a máquina seja dócil o suficiente para nos dizer como mantê-la sob controle (Good, 1965, p. 33).

A advertência acima, embora originalmente formulada em contexto teórico, revela um aspecto central do debate contemporâneo: quanto maior a autonomia operacional das máquinas, maior se torna a dificuldade de controle jurídico sobre os efeitos concretos de sua atuação. No campo das relações de trabalho, isso se manifesta quando sistemas automatizados classificam trabalhadores, projetam riscos de desligamento, monitoram produtividade em tempo real ou realizam triagens de contratação sem transparência suficiente para que a pessoa afetada compreenda os critérios utilizados. O dano, nesse contexto, não decorre necessariamente de uma falha mecânica visível, mas de uma decisão automatizada capaz de gerar exclusão, discriminação, perda salarial, exposição indevida de dados ou intensificação abusiva das condições laborais (Delgado, 2020).

Os prejuízos causados por sistemas de inteligência artificial no trabalho não se limitam a danos patrimoniais. Há também lesões relacionadas à honra, à intimidade, à privacidade, à igualdade de tratamento, à saúde mental e à dignidade do trabalhador, especialmente quando o monitoramento digital permanente converte o ambiente de trabalho em espaço de vigilância contínua. Nessas hipóteses, a tecnologia deixa de ser mero instrumento operacional e passa a integrar a própria estrutura de comando empresarial, razão pela qual o empregador não pode alegar neutralidade tecnológica para afastar sua responsabilidade. O uso da automação como mecanismo de gestão implica, inevitavelmente, a assunção dos riscos jurídicos decorrentes de sua implementação (Pinheiro, 2020).

Nesse sentido, merece destaque a reflexão crítica formulada por Zuboff ao conceituar a lógica contemporânea de exploração de dados e vigilância algorítmica, ao afirmar que:

[...]Uma nova ordem econômica que reivindica a experiência humana como matéria-prima gratuita para práticas comerciais dissimuladas de extração, previsão e vendas; uma lógica econômica parasítica na qual

a produção de bens e serviços é subordinada a uma nova arquitetura global de modificação de comportamento; uma mutação do capitalismo marcada por concentrações de riqueza, conhecimento e poder sem precedentes na história da humanidade; uma ameaça significativa para a natureza humana no século XXI; a origem de um novo poder instrumentário que reivindica domínio sobre a sociedade; uma expropriação de direitos humanos críticos que pode ser compreendida como uma destituição da soberania dos indivíduos (Zuboff, 2020, p. 26).

É possível compreender que o problema da inteligência artificial não reside apenas na eficiência tecnológica, mas no fato de que sistemas automatizados podem ser utilizados como instrumentos de classificação, previsão e modulação de comportamentos humanos em larga escala. Quando esse modelo é aplicado às relações de trabalho, o trabalhador deixa de ser visto apenas como sujeito de direitos e passa a ser tratado como fonte contínua de dados, objeto de análise estatística e elemento ajustável dentro de métricas algorítmicas de desempenho. Tal lógica amplia o risco de danos invisíveis, cumulativos e muitas vezes de difícil comprovação imediata, exigindo do Direito uma resposta preventiva e reparatória ao mesmo tempo.

Outro aspecto sensível diz respeito ao nexo causal. Em diversas situações, empresas buscam diluir a responsabilidade afirmando que determinada decisão foi tomada “automaticamente pelo sistema”, como se a existência do algoritmo fosse suficiente para romper o vínculo entre a atividade empresarial e o dano produzido. Todavia, essa tese não se sustenta juridicamente, pois a inteligência artificial não atua de forma espontânea no mundo social; ela é inserida, parametrizada, alimentada e utilizada dentro de finalidades econômicas específicas. O algoritmo não possui autonomia jurídica, razão pela qual sua atuação deve ser compreendida como extensão da estrutura empresarial que o colocou em funcionamento, especialmente quando seus efeitos atingem direitos fundamentais de trabalhadores (Brasil, 1988).

Assim, a responsabilidade civil aplicada aos danos decorrentes da inteligência artificial deve ser interpretada à luz da teoria do risco da atividade, sobretudo quando a automação integra o núcleo produtivo da empresa e produz vantagens econômicas diretas ao empregador. Quem obtém benefício econômico com a tecnologia também deve suportar os riscos que dela decorrem.

A inovação tecnológica, portanto, não pode ser compreendida como zona livre de responsabilidade, mas como atividade submetida aos mesmos deveres jurídicos de cautela, transparência, supervisão e reparação que incidem sobre qualquer prática empresarial potencialmente lesiva. Em um cenário de crescente automação das relações de trabalho, a responsabilidade civil assume não apenas função reparatória, mas também papel preventivo, limitando abusos e reafirmando que o avanço tecnológico não pode se sobrepor à dignidade da pessoa humana (Bittar, 2005).

2.5. Transparência Algorítmica, Explicabilidade e o Direito de Contestação nas Decisões Automatizadas

A crescente utilização da inteligência artificial em processos decisórios trouxe ao debate jurídico uma questão central para a proteção de direitos fundamentais: a opacidade dos sistemas automatizados. Diferentemente das decisões humanas tradicionais, em que é possível identificar critérios, fundamentos e responsáveis, muitas decisões produzidas por algoritmos operam dentro de estruturas técnicas complexas e de difícil compreensão, tornando praticamente invisível o caminho lógico percorrido até o resultado final. Esse fenômeno, conhecido como “caixa-preta algorítmica”, cria um dos maiores desafios regulatórios da atualidade, pois decisões capazes de afetar empregos, salários, admissões, promoções, desligamentos e direitos sociais passam a ser tomadas sem transparência suficiente para que o indivíduo afetado compreenda ou conteste os critérios utilizados (Pinheiro, 2020).

No ambiente das relações de trabalho, esse problema assume proporções ainda mais graves porque a decisão automatizada não é meramente informativa, mas pode produzir efeitos concretos sobre a vida do trabalhador. Sistemas de recrutamento filtram currículos, algoritmos classificam produtividade, softwares avaliam desempenho, plataformas definem ranqueamentos internos e mecanismos digitais podem até determinar bloqueios ou desligamentos automáticos. O trabalhador, contudo, na maioria das vezes, não tem acesso aos

critérios objetivos que motivaram tais decisões, tampouco consegue verificar se houve erro, viés, discriminação ou falha no processamento de seus dados. A ausência de transparência, nesse contexto, compromete não apenas a confiança na tecnologia, mas o próprio exercício do contraditório e da ampla defesa em situações que afetam direitos fundamentais.

A doutrina contemporânea tem alertado que a inteligência artificial não pode operar em ambiente decisório completamente opaco, sobretudo quando produz impactos jurídicos relevantes sobre pessoas. Sobre essa preocupação, destaca-se importante reflexão segundo a qual:

[...] algoritmos analisam dados e são usados para tomar decisões que afetam diretamente a sociedade. Nem sempre os problemas decorrem de intenção deliberada, mas do fato de que o sistema entrega exatamente aquilo que foi programado ou aprendido a partir dos dados recebidos, podendo reproduzir injustiças, vieses e resultados socialmente inadequados se não houver mecanismos de supervisão, correção e transparência desde sua concepção (Kearns; Roth, 2020, p. 18).

A reflexão acima demonstra que a transparência algorítmica não é mero detalhe técnico, mas condição indispensável para a legitimidade jurídica da decisão automatizada. Se um sistema produz efeitos sobre direitos de alguém, esse alguém precisa ter meios mínimos de compreender os critérios que levaram àquela decisão, especialmente quando há risco de erro, discriminação ou dano.

No ordenamento jurídico brasileiro, a Lei Geral de Proteção de Dados trouxe importante avanço ao reconhecer o direito de revisão de decisões tomadas exclusivamente com base em tratamento automatizado de dados pessoais. O artigo 20 da LGPD representa um marco relevante ao estabelecer que o titular dos dados pode solicitar informações claras sobre os critérios e procedimentos utilizados na decisão automatizada, especialmente quando ela afeta interesses jurídicos relevantes. Ainda que a aplicação prática desse dispositivo ainda enfrente limitações, sua existência demonstra que o Direito brasileiro já reconhece que decisões automatizadas não podem operar em absoluta inacessibilidade técnica (Lei nº 13.709/2018).

O problema, contudo, não se resolve apenas com previsão legal abstrata. A dificuldade prática reside justamente no fato de que muitos sistemas de

inteligência artificial, sobretudo aqueles baseados em *machine learning*, desenvolvem padrões internos cuja lógica se torna extremamente difícil de explicar até mesmo para seus programadores. Isso gera um conflito entre eficiência tecnológica e exigência jurídica de explicabilidade. Do ponto de vista do Direito, entretanto, a complexidade técnica não pode ser utilizada como justificativa para afastar garantias fundamentais, pois a dificuldade de explicar uma decisão não elimina seus efeitos concretos sobre quem a sofre.

Essa preocupação é reforçada quando se observa que a ausência de transparência pode transformar a decisão automatizada em verdadeiro mecanismo de poder incontestável. Como adverte Zuboff ao tratar das estruturas contemporâneas de vigilância e modulação comportamental:

[...] uma nova arquitetura de poder baseada na coleta, previsão e modificação de comportamentos humanos opera por meio de mecanismos tecnológicos que concentram conhecimento e capacidade decisória em estruturas inacessíveis à maioria das pessoas, comprometendo a autonomia individual e ampliando formas silenciosas de controle social (Zuboff, 2020, p. 26).

No campo trabalhista, essa lógica se manifesta quando o trabalhador é submetido a decisões automatizadas sem saber como foi avaliado, por que perdeu pontuação, por qual razão foi bloqueado de determinada plataforma ou com base em quais dados teve seu desempenho classificado negativamente. A opacidade algorítmica, nesses casos, não é apenas problema técnico, mas violação potencial de direitos fundamentais relacionados à informação, igualdade, dignidade e defesa.

Por essa razão, a doutrina e a jurisprudência contemporâneas vêm defendendo que sistemas de inteligência artificial utilizados em decisões relevantes devem obedecer a princípios mínimos de transparência, auditabilidade, explicabilidade e possibilidade de contestação. O indivíduo afetado por decisão automatizada precisa ter acesso não necessariamente ao código-fonte integral, mas ao racional decisório mínimo capaz de permitir compreensão, revisão e contestação do resultado produzido.

3. ALGORITMOS, CONTROLE SOCIAL E CAPITALISMO DE VIGILÂNCIA

A Inteligência Artificial apresenta nuances utópicas e distópicas em diversos setores e, em sua aplicação prática, o uso dos algoritmos conseguem responder a qualquer questionamento existente com a base de dados hoje existente. Kearns e Roth (2020) afirmam que, além de preocupações com privacidade, violações de equidade e demais direitos fundamentais, algoritmos vem analisando nossos dados assim como são usados para fazer decisões que afetam a sociedade. Não necessariamente, as violações ocorridas com algoritmos sejam propositais, o que ocorre é que, por padrão, o algoritmo entregará apenas o que lhe foi expressamente solicitado, não necessariamente o que seu *designer* busca. O uso de *machine learning*, quando parametrizadas e em fase de personalização das predições, tais predições podem ser imbuídas de vieses, o que exige ajustes nos algoritmos existentes para que não sejam utilizados como ferramentas discriminatórias, como é o caso do uso policial, onde é possível que a I.A. seja tendenciosa a grupos raciais.

As implicações do uso e do autodesenvolvimento de IAs são levadas em consideração e apontadas por diversas pessoas influentes, como Stephen Hawking, onde afirmou em entrevista à BBC que "o desenvolvimento da inteligência artificial completa pode significar o fim da raça humana" (Cellan-Jonas), no que Elon Musk concorda ao afirmar em entrevista para o The Guardian "Se eu tivesse que adivinhar qual é a nossa maior ameaça existencial, provavelmente é isso [I.A.]" (Gibbs). Tais posicionamentos teriam como base a premissa de que as IAs, em seu autodesenvolvimento, se tornariam superinteligentes em um passo não páreo para o desenvolvimento humano, o que levaria à "explosão de inteligência", conforme concebido por I. J. Good em 1965, onde:

Deixe que uma máquina ultra-inteligente seja definida como uma máquina que pode ultrapassar de longe todas as atividades intelectuais de qualquer homem, por mais inteligente que seja. Uma vez que a concepção de máquinas é uma destas atividades intelectuais, uma máquina ultra-inteligente poderia conceber máquinas ainda melhores; haveria então inquestionavelmente uma "explosão de inteligência", e a inteligência do homem seria deixada muito para trás. Assim, a primeira máquina ultra-inteligente é a última invenção que o homem precisa

fazer, desde que a máquina seja dócil o suficiente para nos dizer como mantê-la sob controle (Good, 1965, p. 33).

Veja que, para tais tecnologias, as soluções tradicionais seriam novas leis e regulamentações, assim como ocorreu com a Lei Geral de Proteção de Dados. Todavia, não é a única frente a ser explorada. Em paralelo com o vanguardismo frente a situações tecnológicas no ordenamento jurídico, é importante coalizar conceitos de moralidade, equidade, privacidade e outros valores sociais de forma a criar novos algoritmos (e, por consequência, Inteligências Artificiais) sem vieses prejudiciais à minorias, ou que seus danos sejam drasticamente reduzidos e de mais fácil reparação. Em razão do exposto, é importante que a preocupação algorítmica, desde sua concepção em atividades menores até a sua explosão de inteligência, devem ser antecipadas de forma a otimizar os efeitos colaterais do uso indevido das IAs (Kerns e Roth, 2020).

Para a presente reflexão, é essencial que sejam levantados alguns conceitos-chave para o fiel andamento do projeto, sendo eles o controle social e o capitalismo de vigilância, ambos adequados à discussão.

O controle social, apesar de parecer simples, possui mais de uma forma, sendo que as principais são o controle sobre a sociedade, onde se busca a garantia da ordem e da coesão social, assim como dominação e poder sobre a maioria, pelo Estado, para assegurar hegemonia nas esferas público-privadas, e o controle da sociedade, onde é forma de exercício da cidadania da sociedade para que controle as atividades estatais de forma ampla, garantindo a democracia. Para este trabalho, o conceito utilizado será o controle social sobre a sociedade, na qual se utiliza como meio de ordem social, dominação e poder sobre os indivíduos (Silva, 2016).

O capitalismo de vigilância, por sua vez, no qual ocorre hoje e que muitas vezes não é percebido pela sociedade, se concretiza ao tornar seres humanos, os cidadãos de todo o mundo, como o mineral que leva instituições públicas ou privadas a alcançarem seus objetivos, em princípio lucrativos. A professora emérita Shoshana Zuboff (2019), criou uma definição ampla para tal capitalismo de vigilância, *in literis*:

1. Uma nova ordem econômica que reivindica a experiência humana como matéria-prima gratuita para práticas comerciais dissimuladas de extração, previsão e vendas; 2. Uma lógica econômica parasítica na qual a produção de bens e serviços é subordinada a uma nova arquitetura global de modificação de comportamento; 3. Uma funesta mutação do capitalismo marcada por concentrações de riqueza, conhecimento e poder sem precedentes na história da humanidade; 4. A estrutura que serve de base para a economia de vigilância; 5. Uma ameaça tão significativa para a natureza humana no século XXI quanto foi o capitalismo industrial para o mundo natural nos séculos XIX e XX; 6. A origem de um novo poder instrumentário que reivindica domínio sobre a sociedade e apresenta desafios surpreendentes para a democracia de mercado; 7. Um movimento que visa impor uma nova ordem coletiva baseada em certeza total; 8. Uma expropriação de direitos humanos críticos que pode ser mais bem compreendida como um golpe vindo de cima: uma destituição da soberania dos indivíduos (Zuboff, 2019, p. 26).

Veja que, como capitalismo de vigilância, se desenha um panorama onde o ser humano, ao trazer diversos *inputs* de dados, sejam eles padrões de personalidade e consumo, interesses socioeconômicos, entre outros, se torna ferramenta para que instituições diversas, sejam públicas ou privadas, possam gerar *insights* e gerar tanto maiores lucros, como também decidir por campanhas políticas com maior efetividade. Não há limites para o uso de tais informações particulares que, em conjunto, podem facilmente definir e identificar pessoas de forma desenfreada.

3.1. Inteligência artificial e controle social: análise de exemplos

A Inteligência Artificial vem sendo aplicada em diversas áreas, desde aplicações para saúde até para o controle social, efetuando uma vigilância constante dos cidadãos baseado na premissa de que melhoram a qualidade de vida. O caso no qual é mais evidente o uso de inteligência artificial para fins de vigilância estatal desgovernada é o que ocorre na China. Em 2014, se iniciou o uso do Social Credit System (ou Sistema de Crédito Social), onde se afirmou pelo governo de que tal sistema é "uma parte importante do sistema econômico de mercado socialista e do sistema de governança social". De fato, o sistema, alimentado por diversos programas amplamente disseminados no país, como o WeChat da Tencent (aplicativo móvel que funciona como uma chave mestra,

sendo uma carteira digital, aplicativo de conversa, market center, entre outros), dados em tempo real da movimentação terrestre via aplicações de GPS como o Beidou, dados bancários chineses, históricos criminais, reconhecimentos faciais em lojas e por câmeras de vigilância públicas, fazem com que, dependendo do comportamento do cidadão chinês, influenciará diretamente no que ele tem acesso. Veja que o sistema não se aplica apenas às pessoas físicas, mas também às pessoas jurídicas.

Um exemplo é que, caso o cidadão, em constante vigilância, cometa alguma infração criminal, ultrapasse um sinal vermelho, fume em uma área proibida, ou mesmo fale mal do governo, poderá ter como resultado desde a diminuição do seu limite de crédito, ter seu pet retirado de sua posse, ter problemas para ser contratado ou entrar em uma universidade, ser proibida a compra de produtos mais luxuosos e até poderá ter bloqueado a compra de voos domésticos, enquanto em contrapartida, os bons cidadãos são recompensados, tendo descontos em diversas contas e/ou produtos do mercado (Canales, 2021).

Apesar de ser o cenário mais distópico e que se utiliza de todas as formas de cruzamento de dados para ter um meio eficaz de controlar a sociedade chinesa, outros países efetuam o uso de tecnologia de modo mais sutil para fins que, ao alcançar os resultados, gera um estado de vigilância e controle social.

Em 2016, foi lançado um programa pelo Serviço de Polícia Metropolitana (Metropolitan Police Service ou MPS) londrino, onde foram instalados duas câmeras, equipadas com inteligência artificial para fins de reconhecimento facial, em pontos movimentados de Kings Cross Central na cidade de Londres. O sistema, com o intuito de assegurar a segurança pública local, colhia imagens de diversas pessoas inocentes e comparava suas imagens com banco de dados contendo uma "lista de vigilância", na qual continham rostos de suspeitos, pessoas desaparecidas e pessoas procuradas pela polícia (Sabbagh, 2019).

Tal sistema se manteve em segredo por 2 anos sem supervisão centralizada, procedimentos e garantias adequadas, encerrando-se em março de 2018, mas levado à público apenas em 2019 através de um Relatório Oficial ao Prefeito de Londres. Nos itens 7 e 9 do relatório oficial enviado ao prefeito informa que as imagens de pessoas que tivessem sido presas, acusadas,

advertidas, repreendidas ou que receberam uma advertência formal eram compartilhadas pela MPS com o Kings Cross Estate Services (composto por Granary Square, Handyside Gardens e Lewis Cubitt Park, St. Pancras Square e Gasholder, bem como todas as estradas de acesso e vias públicas que servem o local) com o intuito de prevenir e detectar crimes, assim como proteger membros da sociedade. Segundo artigo de Sabbagh (2019), é inferido que a base do compartilhamento de dados era ampla demais e autorizava a abordagem arbitrária de inocentes, gerando constrangimento, o que é possível inclusive de ser visto no filme “Coded Bias”, da Netflix.

Outro caso do mau uso da inteligência artificial com fins de controle social foi o caso *Cambridge Analytica*, que chocou o mundo em 2018 ao ter exposto sua influência em diversas campanhas de países do continente africano, como Nigéria e Uganda, no *Brexit* do Reino Unido e, o caso que levou a empresa à mídia, as eleições de 2016 dos Estados Unidos da América. Fornasier e Beck tracejam o que ocorreu na empresa *Cambridge Analytica* (CA) para as eleições americanas que teve êxito em levar Donald Trump à Casa Branca. Tudo começou com o professor de psicologia Aleksandr Kogan, contratado da CA, que criou o aplicativo (app) *itsyourdigitallive* para usar no Facebook. Ao baixar o app, o usuário passava a compartilhar seus dados com a CA, sendo informações pessoais, atividade no Facebook e informações sobre os amigos dos usuários, totalizando cerca de 87 milhões de pessoas com seus dados coletados pela CA.

Com tal base de dados, foi possível que os colaboradores da CA categorizassem os americanos através do software O.C.E.A.N. e, com isso, identificasse eleitores indecisos que poderiam ser levados a considerar votar entre o Partido Republicano ou Democrata, rotulando-os de “os persuadíveis”. Através dessa filtragem, era possível classificar os perfis e efetuar ataques-focais para manipular a opinião política destas pessoas. O Presidente Donald Trump contratou a CA em 2015 para sua propaganda eleitoral e, utilizando de tais ataques-focais e identificando através da IA os Estados decisivos (com maior quantidade de persuadíveis) pela CA, focou sua propaganda eleitoral e saiu vitorioso na corrida presidencial. Em razão da exposição do vazamento de dados, a *Cambridge Analytica* decretou falência em 2018 e, até hoje, o Facebook

sofre com as consequências do uso do aplicativo para tais fins (Fornasier e Beck, 2020).

Em território nacional, é possível identificar algumas aplicações para o uso da inteligência artificial que se enquadram em controle social. No Carnaval de 2019, foram utilizadas câmeras com sistema de reconhecimento facial nas cidades de Salvador/BA e Rio de Janeiro/RJ. Segundo Lisboa (2019), foram instaladas 28 câmeras no bairro de Copacabana durante o carnaval de rua, no qual estava equipado com software da OI, que fazia o congelamento da imagem quando identificado semelhança com o banco de dados, e tal banco de dados fora alimentado com dados da Polícia Civil e Detran, contendo pessoas procuradas pela Justiça (com mandados de prisão em aberto), jovens em cumprimento de medida socioeducativa, assim como dados de veículos roubados/furtados.

Tal operação, mencionada como um teste pela Polícia, teve êxito em localizar e prender 4 pessoas com mandados de prisão em aberto. Um jovem em medida socioeducativa fora identificado e abordado, assim como um veículo roubado foi recuperado com o uso deste software (Lisboa, 2019).

Em Salvador, segundo Alves (2019), ocorreu a primeira prisão bem sucedida da Secretaria de Segurança Pública (SSP-BA) através do reconhecimento facial utilizado em câmeras da cidade. Foram instaladas 44 câmeras com o intuito de identificar armas de fogo e objetos de risco, assim como pessoas com mandado de prisão em aberto, sendo que houve então a identificação e respectiva prisão de um jovem procurado por assassinato desde 2017 (Alves, 2019).

Ainda, segundo Chai e Lima (2020), as operadoras de telefonia móvel nacional geraram dados anonimizados e sigilosos (conforme normas da Medida Provisória 954) de georreferenciamento das pessoas com acesso a tais dispositivos, compartilhados com o Ministério da Ciência, Tecnologia, Inovações e Comunicações. Veja que tais dados anonimizados e randomizados são utilizados para gerar "mapas de calor" e analisar e gerar informações como a efetividade das medidas de prevenção e combate ao coronavírus e a melhor distribuição de recursos de saúde (médicos, equipamentos e medicamentos). O

processamento de tais dados, assim como a emissão de relatórios com os fins adequados ao governo são feitos via inteligência artificial (Chai e Lima, 2020).

3.2. Dos direitos fundamentais e novas tecnologias

A Constituição Federal de 1988 foi uma constituição revolucionária no campo dos direitos humanos, sendo ela o vetor para consolidar diversos direitos e garantias fundamentais, como o direito à vida, moradia, dignidade, entre outros. À sua época, a evolução tecnológica ainda era lenta e limitada, se comparada com o que se encontra disponível nos dias atuais. Apesar de visar assegurar direitos, alguns dos direitos fundamentais acabam por se encontrarem em violação quando utilizada a tecnologia e, por conseguinte, a Inteligência Artificial, como nos exemplos anteriormente expostos.

Os direitos à liberdade e privacidade estão previstos no art. 5º da Constituição Federal de 1988 e são considerados no nosso ordenamento jurídico como cláusulas pétreas. Entretanto, o uso exacerbado da tecnologia e aplicação de inteligências artificiais em meio aos humanos não causa uma violação a estes princípios?

Balkin, Jack (2004) *apud Goulart* afirma que “as novas tecnologias modificam as condições sociais nas quais as pessoas desenvolvem o seu discurso”. Por um lado, a internet trouxe maior diversidade de meios de comunicação e interação entre os usuários, possibilitando uma ampliação do direito de liberdade de expressão, se seguidas as diretrizes das legislações nacionais. Por outro, todos os seus dados estão sendo captados e armazenados num banco de dados de *big data*, ou seja, tudo o que ocorre nos trilhos da internet pode ser rastreado, inclusive há casos de censura e violação da liberdade de expressão por usuários da rede, seja por inteligências artificiais ou por mecanismos humanos.

Desse modo, o direito à privacidade necessita de maiores cuidados para ser assegurado, visto que o atual momento de novas tecnologias é também o momento das maiores violações à privacidade, com o rastreamento de informações e compra e venda de dados em meio à internet (AblasA, 2020)¹⁰.

O direito à igualdade, também previsto no art. 5º da Constituição Federal de 1988, tem como foco tratar as pessoas de modo igualitário, sem distinção de crenças, opiniões, etnias e demais formas de discriminação. Do mesmo modo, as inteligências artificiais são máquinas que foram treinadas para alguma finalidade, dentre elas o reconhecimento de pessoas de ambos os sexos para fins de pesquisa ou específicos.

Um caso bastante emblemático de desigualdade ocasionado por inteligências artificiais ocorreu no ano de 2014, na empresa *Amazon*. Na ocasião, a empresa, a fim de otimizar os serviços de contratação de novos funcionários, adquiriu um software de inteligência artificial para análise de currículos e seleção dos cinco melhores. Em que pese a ideia ser revolucionária, a IA escolhia os melhores candidatos com base nos algoritmos dos funcionários contratados nos últimos 10 anos, sendo na grande maioria, homens. Assim, os currículos que continham a informação “sexo feminino” automaticamente eram discriminados pela IA e, conseqüentemente, não ficaram entre os cinco melhores currículos (Alves, 2018).

Esse caso só demonstra que as inteligências artificiais podem violar o princípio constitucional da igualdade e, para que isso não ocorra, é de extrema importância o debate sobre o impacto da Inteligência Artificial em decisões automatizadas.

Outro direito fundamental é a proteção de dados, recentemente incluída no texto constitucional pelo Congresso Nacional. A Emenda Constitucional nº 115, de 2022, proveniente da PEC nº 17 de 2019, incluiu a proteção de dados pessoais entre aos direitos fundamentais, bem como fixou que a União é competente privativa para legislar sobre proteção e tratamento de dados pessoais, assim como teria as funções de organizar e fiscalizar o tema, nos moldes da lei.

Como direito fundamental, casos internacionais como o vazamento de dados da Cambridge Analytica devem ser revistos nacionalmente para que não haja um dano de ordem constitucional e vazamento de milhões de dados pessoais dos brasileiros.

3.3. Consequências do uso de IA para controle social

Considerando os notórios avanços tecnológicos ocorridos no século XXI, é importante analisar os movimentos da sociedade e sua influência nas responsabilidades civis e penais da inteligência artificial, em especial quando são utilizadas para fins maliciosos de controle social.

Segundo Lévy, Pierre (1999), *apud Chaves Junior* e Berzagui: “[...] não somente as técnicas são imaginadas, fabricadas e reinterpretadas durante seu uso pelos homens, como também é o próprio uso intensivo das ferramentas que constitui a humanidade enquanto tal [...]”. Assim, as constantes mudanças tecnológicas para aprimoramento das IAs são o embate entre a própria finalidade delas em meio aos humanos.

Partindo disso, é possível perceber que a inteligência artificial refere-se à parte da tecnologia que procura estabelecer máquinas capazes de desenvolver tarefas cognitivas normalmente realizadas pelo ser humano. Tais atividades estão relacionadas à resolução de problemas, tendo como base determinadas informações obtidas pela máquina, com a finalidade de que ela seja capaz de chegar a uma conclusão por meios próprios.

A partir dessa conceituação, observa-se que a inteligência artificial pode ser compreendida como um campo tecnológico voltado à criação de sistemas computacionais aptos a reproduzir, simular ou executar funções tradicionalmente associadas à cognição humana, tais como raciocínio, aprendizagem, tomada de decisão, reconhecimento de padrões e processamento de linguagem. Embora a definição apresentada seja sintética, ela evidencia um aspecto central da IA: a tentativa de aproximar a capacidade operacional das máquinas de determinadas competências intelectuais humanas, ainda que por meio de mecanismos algorítmicos distintos da consciência ou da racionalidade biológica. Nesse contexto, a inteligência artificial consolida-se como uma tecnologia estratégica capaz de impactar múltiplos setores da sociedade, desde a automação industrial até áreas sensíveis como saúde, educação, segurança e justiça (Russell; Norvig, 2021).

ao Código Civil, mais precisamente os artigos 186 e 927, visto que tratam sobre o tema. Segundo redação do art. 186 do mesmo diploma legal, “aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito”, bem como o art. 927 impõe uma obrigação em sua redação, visto que descreve que “aquele que, por ato ilícito (arts. 186 e 187), causar dano a outrem, fica obrigado a repará-lo”. O questionamento a ser analisado é sobre quem deve ser responsabilizado (programador, controlador ou quem as de fato utiliza) caso uma IA cometa algum ilícito civil, ou até mesmo um ilícito penal.

No Brasil, o tema ainda é muito recente e, por isso, ainda não existem julgados ou legislações concernentes exclusivamente sobre as consequências e responsabilidade civil por danos causados por inteligências artificiais, mas tão somente no âmbito da Constituição Federal que trata da promoção das inovações tecnológicas pelo Estado (arts. 218 e 219), o que nos remete leva a buscar outras fontes internacionais.

Sobre o tema, existe a Resolução do Parlamento Europeu de 16 de fevereiro de 2017, que tratou sobre diversos assuntos envolvendo a evolução da robótica e inteligência artificial, sendo referência ao Brasil, bem como para diversos outros países que forem carentes de legislação nacional.

Dentre os debates na casa legislativa, foram levantadas as teorias sobre a responsabilização dos criadores, operadores e quem as de fato utiliza, visto que as IAs não surgem por elas mesmas, ou seja, há um grupo de pessoas que transformam a autoaprendizagem em um código a ser reproduzido pela máquina.

Com isso, a Resolução dispõe que deve haver a transparência e a prestação de contas como valores universais, para não afetar o processo de investigação e inovação no desenvolvimento das tecnologias. Ainda, salienta que nos últimos anos os robôs e softwares tiveram uma rápida evolução, culminando com sua interação em massa no ambiente humano.

Partindo dessa análise, consideraram que os robôs estão cada vez mais independentes dos seus criadores e, por isso, não poderiam mais serem vistos

como instrumentos de uso dos humanos, o que levantou a dúvida sobre a responsabilidade para atos causados por autonomia da IA. O grande problema é que na Europa, assim como no Brasil, a legislação atual não permite a responsabilização direta de coisas, mas sim direcionadas a alguma pessoa física ou jurídica, voltando novamente à análise inicial.

Como conclusão do debate, a Resolução trouxe inúmeras considerações, dentre as quais os legisladores elencaram a responsabilidade objetiva para os danos causados por IAs autônomas, como exemplo dos danos causados pelo Estado aos cidadãos. Porém, não especificaram exatamente o responsável, mas atribuíram a maior parcela da culpa ao programador da IA, por este ter sido o responsável pelo código de ativação da atividade do robô. Por fim, chegaram à conclusão de que quanto maior o grau de autonomia da inteligência artificial, maior o grau de responsabilização civil pelo programador.

Desse modo, como no Brasil não há uma lei específica para o caso acima, apenas o Código Civil, é importante que, para os casos concretos envolvendo uma responsabilização por danos causados por IA, seja levada em consideração as diretrizes do Parlamento Europeu, que nitidamente está à frente, a fim de que possamos ter uma melhor resposta à evolução do uso de IAs na responsabilização civil dos danos, especialmente quando da tentativa de controle social.

Por outro lado, não diferentemente da responsabilidade civil, a responsabilidade penal também é algo inerente aos seres humanos, não existindo uma lei para tipificar crimes cometidos por ações autônomas de uma inteligência artificial, mas apenas aquelas em que o ser humano programa a máquina para cometer crimes, de forma dolosa.

Segundo o Código Penal, art. 18, inciso I, diz-se o crime doloso quando o agente quis o resultado ou assumiu o risco de produzi-lo, ou seja, quando o agente agindo com consciência e dolo programa a inteligência artificial para a realização de determinado crime, vindo a responder pelo crime consumado ou pretendido. É a teoria simples e pura adotada pelo nosso ordenamento jurídico, pois a IA foi apenas instrumento de fins maliciosos, não agindo de modo diverso do pretendido.

O grande problema é quando a máquina é programada para agir de modo “x” e acaba agindo de modo “y”, ou seja, contra a vontade previamente estabelecida do seu programador ou usuário. Trata-se, segundo Lima, Taisa Maria Macena (2019), *apud* Chaves Junior e Berzagui, de máquinas que: “[...]ensinam a si próprias novas estratégias e procuram novas evidências para analisar”. São sistemas que se diferenciam justamente pela elevada capacidade de autoaprendizagem grau de independência.

Ainda, segundo a autora, “trata-se de sistemas que podem aprender e executar tarefas sem direção humana ou sem supervisão”, culminando num poder de tomada de decisões sem interferência humana, com resultados consequentemente indesejados pelo desenvolvedor do programa. Nesse caso, a autonomia da IA se traduz em uma lacuna penal na atual legislação, visto que não há lei específica que trata sobre o tema. Sendo assim, fica a dúvida em quem deverá ser o responsável pelo ilícito penal cometido por uma inteligência artificial autônoma.

Dito isso, podemos concluir que o atual Direito Penal não demonstra a viabilidade ou possibilidade de punir um sistema de inteligência artificial, visto que o sujeito ativo do crime deve ser uma pessoa física, dotada de personalidade e sentimentos, os quais formam o dolo de praticar a conduta com consciência da ilicitude.

Assim, caso verificada uma responsabilidade penal, a conduta deverá sempre ser atribuída a um ser humano, nunca à máquina, pois ela não é dotada de sentimentos e intenções objetivas. Logo, essa responsabilidade seria vinculada a uma pessoa humana, de forma culposa ou dolosa, pois é o ser pensante que o cria, altera ou coloca a máquina em funcionamento.

3.4. Desafios Regulatórios e Perspectivas Jurídicas para o Uso da Inteligência Artificial

O avanço da inteligência artificial no ambiente social, econômico e laboral impôs ao Direito um dos maiores desafios regulatórios do século XXI, justamente

porque a velocidade da inovação tecnológica não tem sido acompanhada pela mesma rapidez no desenvolvimento normativo. A expansão de sistemas algorítmicos em áreas sensíveis, como relações de trabalho, segurança pública, consumo, saúde e tomada de decisões automatizadas, evidencia que a ausência de regulação específica não representa neutralidade jurídica, mas sim a criação de espaços de risco onde direitos fundamentais podem ser afetados sem mecanismos adequados de prevenção, controle e responsabilização. Nesse cenário, o debate regulatório deixa de ser uma escolha política opcional e passa a ser uma exigência estrutural de proteção jurídica diante do poder crescente das tecnologias inteligentes (Schwab, 2016).

Um dos maiores problemas relacionados à regulação da inteligência artificial é justamente a falsa percepção de que a inovação tecnológica deve operar em ambiente livre de intervenção normativa para não comprometer o progresso científico. Essa lógica, embora sedutora sob a ótica econômica, ignora que toda tecnologia inserida em sociedade produz efeitos jurídicos, sociais e humanos. A ausência de regulação não elimina riscos, mas apenas transfere seus custos para indivíduos vulneráveis, trabalhadores, consumidores e grupos historicamente marginalizados. Por essa razão, a construção de marcos regulatórios específicos para IA não representa obstáculo ao desenvolvimento, mas instrumento necessário para compatibilizar inovação e proteção de direitos fundamentais (Pinheiro, 2020).

A doutrina internacional já vem alertando para esse problema ao demonstrar que algoritmos não são neutros, pois refletem bases de dados, escolhas de programação e objetivos previamente definidos por agentes humanos. Como observam Kearns e Roth:

[...]Além das preocupações com privacidade, violações de equidade e demais direitos fundamentais, algoritmos analisam dados e são usados para tomar decisões que afetam diretamente a sociedade. Nem sempre as violações algorítmicas decorrem de intenção deliberada, mas muitas vezes surgem porque o algoritmo entrega exatamente aquilo que foi solicitado, e não necessariamente aquilo que seria justo ou socialmente adequado, exigindo correções e controles para evitar discriminações e danos estruturais (Kearns; Roth, 2020, p. 18).

Essa reflexão demonstra que a inteligência artificial não pode ser tratada apenas como ferramenta técnica, pois seus efeitos ultrapassam o campo computacional e alcançam diretamente a esfera jurídica. Um algoritmo que classifica pessoas, define riscos, seleciona candidatos, monitora trabalhadores ou reconhece rostos não está apenas “processando dados”; está interferindo em direitos, oportunidades e liberdades. Por isso, a regulação da IA deve incorporar princípios de transparência, explicabilidade, auditabilidade, supervisão humana e responsabilização jurídica, evitando que decisões automatizadas se convertam em zonas opacas de poder incontestável.

No cenário europeu, uma das referências mais relevantes para esse debate foi a Resolução do Parlamento Europeu de 2017 sobre robótica e inteligência artificial, que chamou atenção para a necessidade de construção de mecanismos de responsabilidade, prestação de contas e controle normativo sobre tecnologias autônomas. O documento partiu da premissa de que o avanço da autonomia tecnológica não pode afastar a imputação jurídica quando houver dano, razão pela qual passou a discutir critérios de responsabilidade objetiva e deveres de supervisão relacionados ao uso de sistemas inteligentes (Parlamento Europeu, 2017). Embora não resolva integralmente a questão, o debate europeu tornou-se paradigma internacional por reconhecer que a inteligência artificial exige respostas jurídicas próprias e não pode ser enquadrada apenas em modelos clássicos sem adaptações.

No Brasil, a situação ainda é marcada por fragmentação normativa. Existem regras relacionadas à proteção de dados, direitos fundamentais, responsabilidade civil e defesa do consumidor, mas não há ainda um sistema plenamente consolidado de regulação da inteligência artificial capaz de enfrentar de forma específica questões como decisões automatizadas, danos algorítmicos, discriminação sistêmica, responsabilidade por falhas autônomas e limites ao uso de IA em ambientes laborais e estatais. Essa lacuna normativa amplia a insegurança jurídica e deixa trabalhadores e cidadãos expostos a mecanismos tecnológicos que operam muitas vezes sem transparência ou fiscalização adequada (Brasil, 1988).

Nesse sentido, merece atenção a advertência de Zuboff ao afirmar que a vigilância digital e o uso massivo de dados não representam apenas inovação econômica, mas uma reconfiguração das relações de poder na sociedade contemporânea. Segundo a autora:

[...] capitalismo de vigilância reivindica domínio sobre a sociedade por meio da extração contínua de dados e da modificação comportamental em larga escala, criando uma nova ordem de poder baseada em previsões, controle e intervenções sobre a experiência humana, de modo que a própria soberania dos indivíduos passa a ser ameaçada por estruturas tecnológicas que operam acima da compreensão comum (Zuboff, 2020, p. 26).

A preocupação exposta pela autora revela que a regulação da inteligência artificial não deve se limitar à correção de falhas técnicas, mas precisa enfrentar o problema estrutural da concentração de poder informacional e decisório em sistemas algorítmicos de larga escala. No campo das relações de trabalho, isso se torna ainda mais sensível, pois a ausência de regras claras pode transformar o trabalhador em objeto permanente de vigilância, classificação e controle automatizado, submetido a decisões invisíveis sem possibilidade real de contestação.

Diante desse cenário, a perspectiva jurídica contemporânea aponta para a necessidade de construção de um modelo regulatório baseado em princípios fundamentais: supervisão humana significativa, transparência algorítmica, proibição de discriminação automatizada, proteção de dados pessoais, responsabilização objetiva em casos de danos relevantes e mecanismos efetivos de auditoria tecnológica. Não se trata de impedir o avanço da inteligência artificial, mas de assegurar que sua utilização ocorra dentro de parâmetros jurídicos compatíveis com a dignidade da pessoa humana e com os fundamentos do Estado Democrático de Direito. A inovação tecnológica, quando desacompanhada de regulação, pode se transformar em instrumento de exclusão, vigilância e violação de direitos; quando juridicamente controlada, pode ser integrada ao desenvolvimento social de forma legítima e segura (Pinheiro, 2020).

3.5. Responsabilidade Civil e Penal pelo Uso Indevido da Inteligência Artificial no Controle Social

O uso crescente da inteligência artificial como ferramenta de monitoramento, classificação, vigilância e tomada de decisões em larga escala trouxe ao debate jurídico contemporâneo uma questão de extrema relevância: a responsabilização pelos danos causados quando tais sistemas são utilizados de forma indevida ou produzem resultados lesivos aos indivíduos. Embora a inteligência artificial seja frequentemente apresentada como mecanismo de eficiência, neutralidade e precisão, sua aplicação prática demonstra que sistemas automatizados podem produzir violações à privacidade, discriminações estruturais, constrangimentos indevidos, danos morais, prejuízos patrimoniais e até impactos em direitos fundamentais de liberdade, igualdade e dignidade. Diante disso, o Direito passa a enfrentar a necessidade de definir quem deve responder quando a tecnologia deixa de ser instrumento de inovação e passa a produzir consequências ilícitas (Bittar, 2005).

No campo da responsabilidade civil, a discussão gira em torno da imputação jurídica dos danos produzidos por sistemas automatizados, especialmente quando a inteligência artificial atua em contextos de vigilância social, reconhecimento facial, análise comportamental, classificação de risco ou monitoramento digital em massa. O problema central está no fato de que a inteligência artificial não possui personalidade jurídica própria, razão pela qual não pode ser diretamente responsabilizada. Assim, eventual dano deverá ser juridicamente atribuído à pessoa física ou jurídica que desenvolveu, programou, implementou, comercializou ou utilizou o sistema de forma lesiva, observando-se os critérios de causalidade, dever de cautela e risco da atividade (Santos, 2020).

A doutrina contemporânea já advertia, inclusive em estágios iniciais da discussão sobre autonomia das máquinas, que o avanço da inteligência artificial exigiria mecanismos prévios de controle. Sobre esse ponto, destaca-se importante reflexão clássica:

[...] a primeira máquina ultra-inteligente é a última invenção que o homem precisa fazer, desde que a máquina seja dócil o suficiente para nos dizer como

mantê-la sob controle. Uma vez que uma máquina possa ultrapassar a capacidade intelectual humana e produzir novas soluções por conta própria, o problema central deixa de ser apenas sua criação e passa a ser justamente a capacidade humana de controlar seus efeitos (Good, 1965, p. 33).

A advertência acima demonstra que o debate jurídico não se concentra apenas na criação tecnológica, mas principalmente no controle de seus efeitos concretos. Quando a inteligência artificial é utilizada em contextos de controle social, como reconhecimento facial, vigilância urbana, rastreamento de dados ou análise preditiva de comportamento, o risco de danos se amplia significativamente, pois decisões automatizadas podem atingir milhares de pessoas simultaneamente, produzindo impactos individuais e coletivos de grande magnitude.

No campo da responsabilidade civil, a teoria do risco da atividade ganha relevância justamente porque empresas e instituições que se beneficiam economicamente ou funcionalmente da inteligência artificial assumem também os riscos decorrentes de sua utilização. Se uma tecnologia é implementada para gerar lucro, otimizar serviços, ampliar controle ou automatizar decisões, os danos eventualmente produzidos não podem ser tratados como meras falhas neutras da máquina, mas como consequências juridicamente vinculadas à atividade de quem a colocou em funcionamento. O algoritmo não rompe, por si só, o nexos causal entre a conduta empresarial e o dano causado ao indivíduo.

Essa preocupação se torna especialmente relevante em contextos de vigilância e monitoramento em massa. Como aponta a crítica doutrinária ao capitalismo de vigilância:

[...] uma nova ordem econômica reivindica a experiência humana como matéria-prima gratuita para práticas de extração, previsão e modificação comportamental, concentrando poder e criando mecanismos de intervenção sobre indivíduos em escala inédita, com riscos reais à autonomia, à privacidade e à liberdade (Zuboff, 2020, p. 26).

A reflexão acima evidencia que o uso indevido da inteligência artificial pode ultrapassar o campo do dano individual e atingir a própria estrutura de direitos fundamentais em sociedade. O controle algorítmico, quando aplicado sem limites, pode gerar discriminação automatizada, exclusão de oportunidades,

exposição indevida de dados, perseguição comportamental, vigilância abusiva e constrangimentos incompatíveis com o Estado Democrático de Direito.

No campo penal, o debate assume contornos ainda mais complexos. O Direito Penal brasileiro estrutura-se sobre a ideia de conduta humana consciente, típica, antijurídica e culpável, razão pela qual a inteligência artificial, por não possuir vontade jurídica, consciência moral ou capacidade de culpabilidade, não pode ser considerada sujeito ativo de crime. A máquina não age com dolo ou culpa em sentido jurídico; ela executa comandos, aprende padrões e produz resultados dentro de sua programação e capacidade operacional. Assim, eventual responsabilidade penal deverá recair sobre seres humanos envolvidos na criação, programação, utilização ou emprego doloso ou culposos da tecnologia em contexto criminoso (Código Penal, art. 18).

Quando a inteligência artificial é deliberadamente utilizada como instrumento para prática de crimes, como invasão de sistemas, perseguição digital, manipulação de dados, disseminação de conteúdos ilícitos, monitoramento abusivo ou fraude, a responsabilização penal continua recaindo sobre a pessoa humana que utilizou a tecnologia como meio de execução da conduta criminosa. Nesse caso, a máquina atua como instrumento, e não como sujeito penal.

O problema mais complexo surge quando sistemas altamente autônomos produzem resultados não previstos por seus programadores, especialmente em contextos de autoaprendizagem, adaptação contínua e tomada de decisão automatizada sem supervisão imediata. Ainda que a autonomia técnica aumente, o ordenamento jurídico brasileiro não admite a punição penal da máquina, razão pela qual a análise continua recaindo sobre eventual falha humana na programação, ausência de cautela, negligência na supervisão ou dolo na implementação de sistemas perigosos.

Dessa forma, tanto na responsabilidade civil quanto na responsabilidade penal, a inteligência artificial não elimina a centralidade da responsabilidade humana. A tecnologia pode sofisticar a forma de ocorrência do dano, ampliar sua escala ou dificultar sua rastreabilidade, mas não afasta a necessidade de imputação jurídica a pessoas físicas ou jurídicas que, direta ou indiretamente,

deram causa ao resultado lesivo. Portanto, a inteligência artificial não pode ser tratada como espaço de irresponsabilidade normativa, pois seu uso deve permanecer subordinado aos princípios da dignidade da pessoa humana, da proteção de direitos fundamentais e da responsabilização jurídica pelos danos causados em sociedade.

4. DECISÕES AUTOMATIZADAS E LIMITES DA CLT

A Consolidação das Leis do Trabalho foi desenhada para uma realidade industrial do século passado. O avanço da IA e da automação, porém, desafia seus institutos centrais: subordinação, jornada, remuneração e responsabilidade empregatícia. O artigo 20 da LGPD exige revisão profunda das práticas empresariais, mas a CLT não prevê critérios objetivos para decisões baseadas em algoritmos, nem mecanismos de defesa efetiva para trabalhadores prejudicados por decisões automatizadas (Delgado, 2020).

Julgados recentes do Tribunal Superior do Trabalho demonstram a dificuldade de enquadrar relações mediadas por plataformas digitais e sistemas de IA nos conceitos tradicionais de vínculo de emprego. As teses de “subordinação algorítmica” e “trabalho em plataformas” vêm sendo reconhecidas em decisões paradigmáticas, mas o direito positivo avança lentamente frente à velocidade da inovação tecnológica (Brasil, 2023).

Doutrinadores defendem que o futuro da CLT depende da incorporação de critérios de explicabilidade algorítmica, proteção contra decisões automatizadas injustas e mecanismos de reparação célere em casos de discriminação digital. Sem isso, o trabalhador fica à mercê de sistemas opacos e de interesses corporativos invisíveis à regulação estatal (Fonseca, 2021).

4.1. Jurisprudência, Legislação e Tendências Regulatórias

A jurisprudência trabalhista nacional começa a responder ao avanço da automação e da IA, ainda que timidamente. Decisões recentes do TST reconhecem vínculo empregatício em relações mediadas por aplicativos de delivery, mesmo diante de estruturas jurídicas criadas para ocultar a relação de emprego (Brasil, TST, 2023). O Ministério Público do Trabalho tem atuado para garantir a aplicação da LGPD em contextos de seleção, monitoramento e gestão digital de trabalhadores (MPT, 2022).

No plano internacional, a União Europeia aprovou diretrizes rígidas sobre decisões automatizadas, direito à explicação e proteção contra discriminação algorítmica, exigindo mecanismos de auditabilidade e responsabilização dos controladores de dados (Rapôso et al., 2019). O Brasil, apesar dos avanços normativos, ainda carece de uma lei específica que regule o uso de IA no trabalho e estabeleça critérios para decisões automatizadas.

Projetos de lei em tramitação propõem a criação de marcos regulatórios para IA, com foco em direitos digitais, transparência, e proteção contra riscos emergentes. A tendência é a convergência das agendas de trabalho, direitos digitais e proteção de dados, sob pena de obsolescência do direito do trabalho diante do avanço tecnológico.

O avanço das plataformas digitais de trabalho provocou uma profunda transformação na forma de prestação de serviços e, conseqüentemente, reacendeu o debate jurídico sobre a configuração do vínculo empregatício em modelos mediados por aplicativos e sistemas automatizados. Durante muito tempo, empresas de tecnologia sustentaram a tese de que atuavam apenas como intermediadoras entre usuários e prestadores de serviço, afastando qualquer responsabilidade típica da relação empregatícia. Contudo, a evolução da jurisprudência trabalhista e da doutrina passou a demonstrar que a ausência de chefia presencial não significa inexistência de subordinação, sobretudo quando o poder diretivo é exercido por mecanismos digitais, algoritmos, softwares de gestão e sistemas automatizados de controle da atividade laboral.

A clássica noção de subordinação jurídica, historicamente vinculada à ideia de ordens diretas, fiscalização humana e inserção física do trabalhador no ambiente produtivo, sofreu significativa releitura diante da economia de plataformas. Isso porque o poder diretivo empresarial deixou de se manifestar apenas por ordens pessoais e passou a operar por meio de comandos automatizados, monitoramento em tempo real, definição de rotas, ranqueamento de desempenho, bloqueios de acesso, precificação dinâmica, distribuição de demandas e sistemas de penalização automatizada. Ainda que não exista contato direto entre gestor e trabalhador, o controle permanece presente, agora exercido em linguagem algorítmica e mediado por tecnologia, revelando uma

nova forma de subordinação compatível com a lógica produtiva da era digital (Delgado, 2020).

Sobre esse ponto, merece destaque importante entendimento jurisprudencial da Justiça do Trabalho, que reconhece a existência de novas formas de subordinação no ambiente tecnológico:

[...] ainda que presente um grau de independência funcional, o elemento subordinação, ainda que diferenciado, subsiste quando o trabalhador está inserido no sistema informático-comunicacional-digital-algoritmo, e que substitui o vetusto critério da inserção material na unidade produtiva. Assim, abstraídas as dimensões espaço-tempo, a hierarquia e a presencialidade, o trabalhador não é um estranho aos interesses vitais da empresa, de organização produtiva e da clientela, que se vale dos instrumentos das novas tecnologias para otimizar o alcance das metas e da produtividade. Logo, o elemento inserção do trabalhador no ciclo produtivo ou na organização telemática, digital-algórica da empresa é critério que assume importância vital caracterizante da *fattispecie* social típica do trabalho subordinado por algoritmo (TRT-2, Processo 1001005-80.2023.5.02.0025, Rel. Ivani Contini Bramante, j. 15 maio 2024).

A decisão acima demonstra que a subordinação contemporânea não pode ser analisada apenas sob parâmetros clássicos de presencialidade e comando humano direto. O trabalhador inserido em plataforma digital não atua de forma plenamente autônoma quando sua atividade depende de conexão contínua com sistema informatizado que determina critérios de funcionamento, remuneração, visibilidade, aceitação de corridas, bloqueios e permanência na atividade. O algoritmo, nesse cenário, não é simples ferramenta tecnológica, mas mecanismo de comando e organização empresarial.

A Constituição Federal de 1988, ao assegurar proteção ao trabalho e estabelecer, no artigo 7º, inciso XXVII, a proteção em face da automação, demonstra que o avanço tecnológico não pode ser utilizado como justificativa para esvaziar garantias trabalhistas historicamente consolidadas. A inovação é juridicamente legítima, mas não pode produzir retrocesso social. O uso de plataformas digitais, aplicativos e inteligência artificial deve ser compatibilizado com os princípios constitucionais da dignidade da pessoa humana, do valor social do trabalho e da função social da atividade econômica, sob pena de se

criar um modelo produtivo tecnologicamente avançado, porém socialmente excludente (Brasil, 1988).

Outro aspecto relevante é que a lógica algorítmica frequentemente produz formas de dependência econômica e tecnológica incompatíveis com a tese de autonomia plena defendida por empresas de plataforma. O trabalhador não define livremente o preço final do serviço, não controla a clientela, não possui acesso à estrutura tecnológica essencial do negócio e pode ser penalizado automaticamente por recusas, avaliações negativas ou desempenho considerado insuficiente pelo sistema. Há, portanto, uma dependência estrutural que extrapola a liberdade contratual formal e aproxima a relação da dinâmica típica do trabalho subordinado (Goldschmidt & Cani, 2022).

Nesse sentido, a jurisprudência trabalhista tem avançado ao reconhecer que a subordinação algorítmica representa atualização do poder diretivo patronal, e não sua extinção. A empresa continua organizando a atividade econômica, definindo parâmetros, controlando a execução do serviço e se beneficiando economicamente da força de trabalho, ainda que utilize software e inteligência artificial como instrumentos de gestão. A tecnologia altera a forma do comando, mas não elimina sua essência jurídica.

A reflexão jurisprudencial sobre o tema também aponta que:

[...] o poder diretivo apresenta-se sob novas formas: controle em tempo real, ostensivo e prévio; controle concomitante; controle a posteriori; controle oculto em qualquer fase da execução do trabalho. Destarte, ainda que presente um grau de independência funcional, subsiste a subordinação quando o trabalhador está inserido no sistema informático, telemático e algorítmico da empresa, sendo o software aplicativo, a dependência tecnológica e a inserção no sistema produtivo elementos caracterizadores da nova subordinação jurídica (TRT-2, Processo 1001005-80.2023.5.02.0025, Rel. Ivani Contini Bramante, j. 15 maio 2024).

Assim, o debate sobre vínculo empregatício em plataformas digitais não pode ser reduzido à aparência contratual construída pelas empresas, mas deve observar a realidade concreta da prestação de serviços, conforme orienta o princípio da primazia da realidade no Direito do Trabalho. A tecnologia não revoga a Constituição, não elimina a proteção social e não afasta

automaticamente a incidência das normas trabalhistas. Ao contrário, quanto mais sofisticados se tornam os mecanismos de controle digital, maior se torna a necessidade de releitura jurídica das relações laborais, de modo a impedir que a inovação tecnológica seja utilizada como instrumento de precarização, exclusão de direitos e esvaziamento da proteção ao trabalho humano (Delgado, 2020).

4.2. Propostas de Atualização Normativa

A literatura jurídica propõe que a atualização do direito do trabalho diante da IA e automação deve se basear em três pilares: transparência algorítmica, responsabilização objetiva dos empregadores pelo uso de IA e revisão dos mecanismos clássicos de proteção. Propostas incluem a exigência de explicação acessível das decisões automatizadas, criação de órgãos de fiscalização algorítmica e reconhecimento do direito à reparação por danos decorrentes de vieses ou falhas em sistemas de IA (De Teffé & Medon, 2020; Fonseca, 2021).

Outras sugestões envolvem a incorporação do direito à desconexão digital, a regulação do uso de big data na gestão de pessoas e a inclusão de direitos digitais no rol de garantias fundamentais dos trabalhadores (Zuboff, 2020; MPT, 2022). O futuro da legislação trabalhista depende de mecanismos de adaptação rápida, revisão contínua dos institutos e fortalecimento das entidades de fiscalização e defesa coletiva.

A reinvenção do direito do trabalho é uma necessidade histórica. A regulação precisa ir além da mera proteção formal, construindo um sistema capaz de enfrentar riscos inéditos e garantir a centralidade da dignidade humana em um mundo dominado por algoritmos.

4.3. A Quarta Revolução Industrial e o Novo Paradigma do Trabalho

A Quarta Revolução Industrial, conceito formulado por Klaus Schwab (2016), representa a fusão de tecnologias digitais, físicas e biológicas, reconfigurando de forma acelerada todos os setores econômicos e sociais. Esse cenário não é futuro, é o presente do mercado global e nacional: robôs colaborativos, inteligência artificial, automação de processos produtivos, big data e machine learning estão na base das transformações que atravessam indústrias, serviços, agricultura e setores criativos. O resultado é um deslocamento massivo das relações tradicionais de trabalho, com criação de novas funções e extinção de milhares de postos historicamente ocupados por humanos.

O Brasil, inserido no capitalismo global, sofre impactos diretos desse fenômeno. Dados do Fórum Econômico Mundial e do IBGE apontam para uma tendência clara de substituição do trabalho manual e repetitivo por sistemas automatizados, acompanhada da explosão de plataformas digitais que mediam atividades econômicas com mínima intervenção humana (Schwab, 2016; Antunes, 2018). O desafio é colossal: como garantir trabalho decente, proteção social e dignidade em um cenário de flexibilidade extrema, fragmentação das relações produtivas e desmaterialização do emprego?

A literatura demonstra que a Quarta Revolução Industrial aprofunda desigualdades históricas, beneficiando setores de alta qualificação tecnológica e marginalizando a maioria dos trabalhadores em funções intermediadas por plataformas e IA. O fenômeno da “uberização” do trabalho, caracterizado pela subordinação algorítmica, ausência de vínculos formais e desproteção social, já é uma realidade consolidada em grandes cidades brasileiras (Zuboff, 2020; Prassl, 2017; Durand, 2021). O direito do trabalho, construído para a fábrica fordista e para a lógica do emprego por tempo indeterminado, enfrenta obsolescência acelerada diante do modelo “on-demand” e da economia de dados.

A chamada “sociedade 5.0”, defendida por teóricos contemporâneos, propõe o uso da tecnologia para promover inclusão, sustentabilidade e qualidade

de vida, colocando o ser humano no centro do processo inovador. No entanto, sem regulação eficaz, o risco é de aprofundamento da precarização, exclusão digital e ampliação da violência algorítmica contra grupos vulneráveis (MPT, 2022; OIT, 2020). A centralidade dos dados, a automação das decisões e a opacidade dos algoritmos impõem a necessidade de reinvenção do direito do trabalho, que precisa migrar do foco exclusivo no contrato formal para a proteção das múltiplas formas de prestação de serviço mediadas por tecnologia.

O modelo fordista, marcado pela padronização, jornada fixa e hierarquia rígida, está sendo substituído pelo paradigma da flexibilidade, da automação e da descentralização. Plataformas como Uber, iFood, 99, Amazon Mechanical Turk e aplicativos de microtarefas exemplificam essa transição, operando na fronteira entre autonomia aparente e subordinação efetiva por algoritmos. O trabalho, nesse contexto, deixa de ser relação entre pessoas e passa a ser mediado por sistemas que controlam, avaliam, punem e recompensam de forma automática, sem transparência nem possibilidade real de contestação.

Na perspectiva crítica, autores como Antunes (2018) e Durand (2021) alertam para o surgimento de um novo proletariado digital, submetido a jornadas fragmentadas, remuneração variável e instabilidade permanente. A “gig economy” cria oportunidades para poucos, mas precariza a maioria. A centralidade dos algoritmos na organização produtiva exige do direito uma resposta urgente, baseada em princípios de transparência, equidade e proteção à dignidade do trabalhador.

O futuro do trabalho não será decidido pela tecnologia, mas pelas escolhas regulatórias feitas agora. Sem uma atualização profunda da legislação, o cenário é de intensificação das desigualdades, marginalização em massa e esvaziamento dos direitos sociais históricos.

4.4. Desafios jurídicos na proteção dos direitos fundamentais do trabalhador

A inteligência artificial e a automação introduzem desafios que o direito do trabalho brasileiro nunca enfrentou. A centralização de decisões em sistemas

algorítmicos coloca em xeque a eficácia dos instrumentos jurídicos tradicionais para proteger o trabalhador. A regulação, ainda baseada em premissas da era industrial, mostra-se insuficiente para garantir direitos fundamentais diante da opacidade, do alcance e da autonomia das novas tecnologias. O risco é real: exclusão, discriminação, precarização e a erosão de garantias históricas.

O primeiro grande obstáculo jurídico é a invisibilidade das decisões automatizadas. A maioria das empresas utiliza algoritmos para recrutamento, avaliação, controle de produtividade e até demissão. Os processos são opacos: o trabalhador não sabe como é avaliado nem tem instrumentos para contestar decisões automatizadas. O artigo 20 da LGPD prevê o direito à revisão de decisões automatizadas, mas a efetividade dessa garantia é mínima. A ausência de mecanismos claros de explicação e transparência coloca o empregado em desvantagem estrutural frente ao empregador, que detém todo o controle sobre os dados e o funcionamento do sistema.

O segundo desafio central é o vazio normativo sobre responsabilidade civil. Quem responde por danos causados por um algoritmo? O empregador? O programador? A plataforma? A doutrina brasileira ainda não encontrou consenso. Bittar (2005), Fonseca (2021) e De Andrade & Faccio (2019) discutem que, em regra, a responsabilidade deve recair sobre quem obtém benefício econômico do trabalho, ou seja, o empregador ou a plataforma. Porém, sem legislação clara, decisões judiciais tendem a ser fragmentadas e imprevisíveis. O risco para o trabalhador é ficar sem reparação por discriminação algorítmica, erros de classificação ou monitoramento abusivo.

Outro ponto crítico é o alargamento dos poderes de vigilância e controle sobre o trabalhador. Plataformas digitais e IA potencializam a vigilância em tempo real: localização, produtividade, tempo online, pausas e interações são monitorados permanentemente. Essa hiper-vigilância, sem limites normativos adequados, representa afronta ao direito à privacidade, ao livre desenvolvimento da personalidade e à saúde mental. Jurisprudência do TST já reconhece o dano moral por monitoramento abusivo, mas a regulação é fragmentada e reativa, não preventiva.

A discriminação algorítmica é outra ameaça urgente. Estudos e casos práticos mostram que sistemas de IA, quando treinados com dados históricos, tendem a reproduzir vieses de gênero, raça, idade e deficiência. O caso da Amazon, que excluía candidatas mulheres, e decisões de plataformas que priorizam perfis específicos, comprovam o potencial excludente dessas ferramentas. O Brasil carece de mecanismos de auditoria, explicabilidade e contestação que permitam identificar e reparar decisões discriminatórias. A CLT, desenhada para relações interpessoais, não atinge os processos automáticos mediados por IA.

A precarização do vínculo de emprego é intensificada pelo avanço das plataformas digitais. Modelos de “autonomia” promovem subordinação algorítmica mascarada, onde o trabalhador tem liberdade formal, mas depende de comandos, avaliações e sanções programadas. O TST já reconheceu o vínculo em casos de entregadores de aplicativo, mas as empresas seguem adaptando contratos para driblar decisões judiciais e manter o modelo precário (TST, 2023). O direito positivo corre atrás de fenômenos que mudam em ritmo tecnológico.

Há, ainda, o desafio da fragmentação sindical e da negociação coletiva. Algoritmos individualizam metas, remuneração e critérios de avaliação, tornando quase impossível a organização coletiva e a atuação sindical efetiva. A legislação sindical brasileira, já enfraquecida por reformas recentes, não prevê proteção específica para trabalhadores em plataformas ou sob controle de IA. O resultado é o isolamento e a impotência do trabalhador frente a uma estrutura de poder tecnocrático.

A proteção de dados pessoais torna-se também eixo fundamental da proteção trabalhista. A inclusão do direito à proteção de dados como direito fundamental (EC 115/2022) e a entrada em vigor da LGPD obrigam o legislador e a Justiça do Trabalho a rever institutos clássicos. O consentimento no trabalho é fictício, já que o empregado não tem poder de escolha real. O empregador coleta, processa e compartilha dados sensíveis sem transparência. A responsabilização por vazamentos, abusos ou discriminação ainda é incipiente.

No plano internacional, a União Europeia avança com regulações como o GDPR e a Diretiva sobre Decisões Automatizadas, exigindo explicabilidade, revisibilidade e auditoria dos sistemas de IA. O Brasil está atrasado. Projetos de lei tramitam, mas o ritmo político e o lobby das empresas atrasam mudanças efetivas. A ausência de uma autoridade de fiscalização e de um regime sancionatório robusto torna o direito inócuo para proteger quem mais precisa. Em síntese, os desafios jurídicos impostos pela automação e IA exigem reinvenção radical da lógica do direito do trabalho:

- I. Inclusão de mecanismos de transparência e revisão das decisões algorítmicas;
- II. Responsabilidade objetiva das plataformas e empregadores;
- III. Proteção reforçada de dados pessoais;
- IV. Reconhecimento da subordinação algorítmica e dos novos vínculos;
- V. Instrumentos coletivos para enfrentar a fragmentação promovida por sistemas digitais.

O direito do trabalho do século XXI precisa abandonar o fetiche do contrato formal e assumir a missão de garantir dignidade, não importa a arquitetura da relação. Se não houver resposta institucional agora, o futuro será de desproteção generalizada, desigualdade estrutural e dominação tecnocrática sobre o trabalhador.

4.5. Futuro da legislação trabalhista: tendências e propostas

A legislação trabalhista brasileira, ancorada na CLT de 1943, está em colapso frente ao avanço irreversível da automação e da inteligência artificial. O modelo regulatório que priorizava o vínculo formal, a hierarquia e a negociação coletiva se tornou disfuncional diante do trabalho mediado por algoritmos, plataformas digitais e sistemas autônomos de gestão. O futuro exige ruptura, não adaptação tímida.

A União Europeia aprovou, em 2023, o AI Act, exigindo transparência, auditoria, rastreabilidade e responsabilidade para aplicações de IA em ambientes laborais. O foco é duplo: proteção do trabalhador e estímulo à inovação ética. Os EUA, China e Reino Unido também avançam em marcos regulatórios para IA, com previsão de sanções pesadas para empresas que discriminem ou exponham trabalhadores a riscos injustificados (Rapôso et al., 2019; De Teffé & Medon, 2020).

O Brasil, até aqui, segue atrasado. Projetos de lei tramitam no Congresso, mas enfrentam resistência de lobbies empresariais e desconhecimento técnico de parte significativa dos legisladores. O máximo alcançado foi a inclusão da proteção de dados como direito fundamental (EC 115/2022) e a entrada em vigor da LGPD, ainda aplicada de modo tímido no universo trabalhista. Decisões recentes do TST e notas do MPT já reconhecem o problema, mas a ausência de lei específica gera insegurança jurídica e favorece a precarização estrutural.

Propostas concretas:

- I. Transparência algorítmica obrigatória: toda decisão automatizada que afete direitos trabalhistas deve ser explicada de modo acessível ao trabalhador, com obrigação legal de revelar critérios, dados utilizados e lógica do algoritmo. A recusa à transparência deve gerar presunção de irregularidade, revertendo o ônus da prova para a empresa.
- II. Responsabilização objetiva dos empregadores e plataformas: danos causados por IA – inclusive discriminação, exclusão, bloqueios injustificados e vazamentos de dados – devem gerar obrigação de indenizar, independentemente de culpa. Empresas que utilizam IA para gestão de pessoas assumem o risco dos efeitos adversos dos sistemas.
- III. Direito à revisão humana e à contestação célere: qualquer decisão relevante tomada por IA (admissão, promoção, punição, demissão, avaliação de produtividade) deve ser passível de revisão humana a pedido do trabalhador. Procedimentos de contestação devem ser gratuitos, céleres e protegidos contra retaliação.

- IV. Auditoria externa e permanente: empresas de médio e grande porte que utilizem sistemas de IA devem ser obrigadas a submeter os algoritmos a auditorias externas, independentes, voltadas a identificar e eliminar vieses discriminatórios, riscos à privacidade e falhas de segurança. O resultado deve ser público e acessível.
- V. Reconhecimento da subordinação algorítmica: legislação deve enquadrar trabalhadores controlados por algoritmos e plataformas digitais como empregados, garantindo acesso pleno aos direitos da CLT, FGTS, previdência e demais benefícios.
- VI. Proteção de dados trabalhistas: uso de dados sensíveis no ambiente de trabalho deve ser restrito ao estritamente necessário, com consentimento real (e não presumido) do trabalhador. Vazamentos e usos indevidos devem gerar multas elevadas e responsabilidade solidária de controladores e processadores.
- VII. Direito à desconexão e proteção da saúde mental: jornadas flexíveis e hiperconectividade devem ser reguladas para garantir pausas, descanso efetivo e proteção contra pressões excessivas por produtividade, inclusive com sanção a empresas que não implementem mecanismos de bem-estar digital.
- VIII. Mecanismos coletivos de defesa: sindicatos e entidades de classe devem ter legitimidade ativa para fiscalizar, auditar e contestar sistemas de IA no ambiente de trabalho, inclusive com direito a acesso irrestrito aos códigos-fonte, quando necessário para investigação de abusos.
- IX. Formação e atualização permanente: inclusão de direitos digitais e literacia algorítmica como conteúdo obrigatório em treinamentos corporativos, cursos de Direito e programas de formação sindical, para garantir que trabalhadores possam compreender e exercer seus direitos.
- X. Criação de autoridade pública de fiscalização algorítmica: órgão técnico e independente, com poder de investigar, sancionar e propor políticas públicas para regular o uso da IA nas relações de trabalho, à semelhança das autoridades de proteção de dados pessoais.

Essas propostas não são futurismo: são o mínimo necessário para evitar a barbárie digital no mercado de trabalho. O futuro da legislação trabalhista será determinado pela capacidade de enfrentar o poder das plataformas, a opacidade algorítmica e a velocidade das transformações tecnológicas.

Se o direito do trabalho permanecer inerte, a consequência será a desintegração de direitos sociais e a consolidação de uma massa de trabalhadores invisíveis, precarizados e controlados por sistemas sobre os quais não têm voz nem defesa. O momento de ruptura é agora. Não existe mais espaço para remendos normativos ou discursos vazios de “modernização”. O futuro exige coragem institucional, inovação regulatória e, acima de tudo, compromisso inegociável com a dignidade do trabalho humano.

4.6. Perspectivas Futuras e a Necessidade de Regulação Jurídica da Inteligência Artificial no Brasil

A consolidação da inteligência artificial como ferramenta de uso cotidiano em relações econômicas, sociais e institucionais impõe ao Direito brasileiro a necessidade de superar abordagens reativas e fragmentadas, adotando uma perspectiva regulatória preventiva, sistêmica e compatível com a complexidade tecnológica contemporânea. O cenário atual demonstra que a inteligência artificial não é mais uma tecnologia de aplicação excepcional ou restrita a setores altamente especializados, mas uma estrutura integrada ao funcionamento de empresas, governos, plataformas digitais, sistemas financeiros, segurança pública e relações de trabalho. Diante disso, a ausência de uma regulamentação específica e suficientemente madura não representa apenas lacuna legislativa, mas risco concreto de ampliação de violações a direitos fundamentais em escala automatizada (Schwab, 2016).

A evolução tecnológica produziu um novo modelo de tomada de decisão, no qual algoritmos passaram a exercer funções que antes dependiam exclusivamente de análise humana. Sistemas automatizados classificam candidatos, definem prioridades de atendimento, identificam padrões de consumo, monitoram comportamentos, avaliam riscos, sugerem punições, filtram conteúdos e até interferem em escolhas políticas e econômicas. O

problema central não reside apenas na existência dessas ferramentas, mas no fato de que tais sistemas operam, muitas vezes, dentro de estruturas de opacidade técnica, sem transparência adequada, sem controle democrático efetivo e sem mecanismos claros de responsabilização em caso de danos. Isso faz com que a inteligência artificial deixe de ser apenas instrumento tecnológico e passe a se tornar também mecanismo de exercício de poder (Zuboff, 2020).

Nesse contexto, a regulação jurídica não pode se limitar a respostas pontuais ou à simples adaptação de normas já existentes, pois a complexidade da inteligência artificial exige construção normativa própria. O desafio brasileiro consiste justamente em desenvolver um marco regulatório capaz de equilibrar inovação, desenvolvimento econômico, competitividade tecnológica e proteção de direitos fundamentais, evitando tanto a ausência regulatória quanto o excesso normativo que inviabilize a pesquisa científica. Trata-se de construir um modelo de governança tecnológica que permita o uso legítimo da IA sem transformar a sociedade em espaço de experimentação descontrolada.

Sobre a necessidade de antecipação regulatória diante dos riscos tecnológicos, destaca-se a reflexão doutrinária segundo a qual:

[...] as preocupações com algoritmos não se restringem à privacidade ou à eficiência computacional, mas alcançam diretamente a equidade, a justiça e a estrutura dos direitos fundamentais, exigindo que o desenho algorítmico seja pensado desde sua concepção para evitar vieses, discriminações e danos sociais que, uma vez automatizados, tornam-se mais difíceis de corrigir posteriormente (Kearns; Roth, 2020, p. 18).

A advertência acima revela que a inteligência artificial não deve ser regulada apenas após a ocorrência do dano, mas desde sua fase de desenvolvimento, implementação e uso prático. Isso significa que princípios como transparência, auditabilidade, supervisão humana, não discriminação, explicabilidade e segurança devem integrar a própria arquitetura tecnológica, funcionando como exigências estruturais e não como medidas corretivas posteriores.

No Brasil, alguns avanços normativos já demonstram preocupação com esse cenário, especialmente no campo da proteção de dados pessoais, após a

entrada em vigor da Lei Geral de Proteção de Dados e da inclusão da proteção de dados como direito fundamental na Constituição Federal. Ainda assim, tais mecanismos, embora importantes, não são suficientes para abarcar toda a complexidade da inteligência artificial, sobretudo em questões relacionadas à autonomia decisória de sistemas inteligentes, responsabilidade civil por danos algorítmicos, impactos trabalhistas, discriminação automatizada e uso de IA pelo poder público. A fragmentação legislativa atual demonstra que o país ainda se encontra em fase de adaptação, sem um regime jurídico integral voltado especificamente para a governança da inteligência artificial (Brasil, 1988).

Outro aspecto essencial para o futuro regulatório brasileiro é o reconhecimento de que a inteligência artificial não produz impactos homogêneos sobre toda a população. Grupos vulneráveis tendem a sofrer de maneira mais intensa os efeitos de decisões automatizadas discriminatórias, especialmente quando algoritmos são alimentados por bases históricas enviesadas ou aplicados em contextos de desigualdade estrutural. Assim, a regulação não pode se limitar à proteção abstrata da tecnologia, mas deve incorporar perspectiva de direitos humanos, justiça social e proteção diferenciada para contextos em que a automação possa reproduzir exclusões históricas (Pinheiro, 2020).

Essa preocupação torna-se ainda mais evidente quando se observa a crescente integração entre inteligência artificial, vigilância digital e controle social. Como alertou Zuboff ao tratar do poder derivado da exploração massiva de dados:

[...] uma nova ordem econômica reivindica a experiência humana como matéria-prima gratuita para práticas de extração, previsão e modificação comportamental, criando estruturas de poder capazes de interferir na autonomia individual, concentrar conhecimento e ampliar mecanismos de controle sobre a sociedade em níveis historicamente inéditos (Zuboff, 2020, p. 26).

A reflexão acima demonstra que o futuro da inteligência artificial não pode ser pensado apenas como questão técnica ou econômica, mas como debate jurídico e político sobre limites do poder tecnológico. O Estado brasileiro, nesse cenário, não pode atuar apenas como incentivador da inovação, mas também como garantidor de direitos fundamentais diante da crescente automação de

decisões e da expansão de mecanismos digitais de vigilância e classificação social.

Diante disso, as perspectivas futuras apontam para a necessidade de um modelo regulatório nacional baseado em governança ética, transparência algorítmica, responsabilização jurídica, proteção de dados, controle democrático e supervisão humana significativa. O desenvolvimento tecnológico continuará avançando de forma acelerada, independentemente da velocidade do Direito. A questão central não é impedir esse avanço, mas assegurar que ele ocorra dentro de limites jurídicos capazes de proteger a dignidade da pessoa humana, a liberdade, a igualdade, a privacidade e a justiça social. Em última análise, o futuro da inteligência artificial no Brasil dependerá não apenas da capacidade técnica de inovação, mas da capacidade jurídica e institucional de impedir que a tecnologia se transforme em instrumento de violação sistemática de direitos.

CONCLUSÃO

A pesquisa evidenciou, de modo inquestionável, que a inteligência artificial e a automação vêm promovendo uma transformação estrutural e irreversível nas relações de trabalho, colocando o direito do trabalho brasileiro diante de um abismo normativo. O objetivo central; analisar os impactos dessas tecnologias sobre as relações normativas e a proteção dos direitos fundamentais dos trabalhadores, foi plenamente atingido ao demonstrar que a legislação vigente, ancorada na CLT e em paradigmas do século XX, tornou-se incapaz de oferecer respostas eficientes frente à explosão do controle algorítmico, à subordinação digital e à desintegração do vínculo formal de emprego.

A pergunta de pesquisa, “Como o direito do trabalho brasileiro pode ser atualizado para assegurar a proteção efetiva dos trabalhadores diante do avanço irreversível da inteligência artificial e da automação?”, foi respondida com precisão: não há saída possível sem uma reinvenção radical do modelo regulatório, fundada na transparência algorítmica, na responsabilização objetiva de empregadores e plataformas, e na garantia efetiva de direitos digitais e proteção de dados pessoais. A hipótese; de que a legislação atual é insuficiente para enfrentar os novos riscos, foi confirmada empiricamente e teoricamente.

O trabalho expôs que a invisibilidade das decisões automatizadas, a ausência de mecanismos de revisão, a fragmentação do vínculo e a precarização estrutural são realidades vividas por milhões de trabalhadores em todo o país. Casos concretos, como o da Amazon e as práticas de plataformas de transporte e entrega, demonstram que os riscos não são potenciais, mas atuais, impactando especialmente grupos historicamente vulneráveis. A precarização, a exclusão algorítmica e o abuso de dados se tornaram faces cotidianas do trabalho digital no Brasil.

A análise comparativa com experiências internacionais revelou que o Brasil está atrasado na formulação de um marco regulatório robusto para inteligência artificial no trabalho. Enquanto União Europeia, EUA e China avançam com legislações específicas e autoridades independentes, a realidade nacional ainda é de tímidos avanços, judicialização dispersa e forte resistência

de setores empresariais. O resultado é insegurança jurídica, perda de direitos e ampliação das desigualdades.

Os pontos fortes deste trabalho residem na abordagem crítica, na identificação dos vazios normativos e na proposição de alternativas jurídicas factíveis. As propostas apresentadas; transparência obrigatória, auditoria externa, responsabilização objetiva, reconhecimento da subordinação algorítmica, proteção de dados trabalhistas e mecanismos coletivos de fiscalização, constituem agenda mínima para evitar o colapso do sistema de proteção social brasileiro diante do avanço da IA.

Os resultados apontam para um cenário claro: ou o direito do trabalho assume a vanguarda regulatória, enfrentando o poder das plataformas e dos sistemas automatizados, ou se tornará irrelevante, condenado a assistir à consolidação da servidão digital e à marginalização em massa dos trabalhadores. Não há neutralidade possível. O futuro é de ruptura; a escolha é entre a dignidade humana e o domínio dos algoritmos.

Recomenda-se, para além da revisão legislativa urgente, a construção de uma autoridade nacional de fiscalização algorítmica, a capacitação de sindicatos e órgãos de fiscalização para lidar com sistemas inteligentes, e o investimento maciço em educação digital para trabalhadores. Sem esses pilares, a assimetria de poder só tende a se ampliar.

O debate sobre inteligência artificial e trabalho não é técnico, é político e ético. O direito do trabalho do século XXI será irrelevante se não for disruptivo. A dignidade do trabalhador depende de coragem institucional e inovação regulatória, não de nostalgia normativa.

REFERÊNCIAS

ABLAS, Barbara. **Como é a venda de informações na Internet?** Veja quanto seus dados valem. Relatório da Kaspersky revela os riscos do vazamento de dados para pessoas anônimas. TechTudo, 2020. Disponível em: <<https://www.techtudo.com.br/listas/2020/12/como-e-a-venda-de-informacoes-na-internet-veja-quanto-seus-dados-valem.ghtml>>. Acesso em: 25 maio.2025.

ALVES, Alain Tiago. **Flagrado por câmera vestido de mulher no carnaval na BA matou homem após vítima passar perto dele de moto em alta velocidade.** Disponível em: <<https://g1.globo.com/ba/bahia/carnaval/2019/noticia/2019/03/07/flagrado-por-camera-vestido-de-mulher-no-carnaval-na-ba-matou-homem-apos-vitima-passar-perto-dele-de-moto-em-alta-velocidade.ghtml>>. Acesso em: 04 jul.2025.

ALVES, Arianne. Uso de algoritmos em análise de currículo pode gerar seleção enviesada. **Exame**, 25/10/2018. Disponível em: <<https://exame.com/tecnologia/uso-de-algoritmos-em-analise-de-curriculo-pode-gerar-selecao-enviesada/>>. Acesso em: 21 maio. 2025

ANTUNES, Ricardo. **O privilégio da servidão:** o novo proletariado de serviços na era digital. São Paulo: Boitempo, 2018.

BITTAR, C. A. **Responsabilidade civil:** teoria e prática. Rio de Janeiro: Forense, 2005.

BOTELHO, Marcos César. A LGPD e a proteção ao tratamento de dados pessoais de crianças e adolescentes. **Revista Direitos Sociais e Políticas Públicas–Unifafibe**, v. 8, . 2, 2020.

BRASIL. **Art. 18 do Código Penal**, Decreto-Lei nº 2.848, de 07 de dezembro de 1940.

BRASIL. Art. 147 do CP, **Decreto Lei 2.848 de 07 de dezembro de 1940.**

BRASIL. Art. 154-A do CP, **Lei 12.737 de 30 de novembro de 2012.**

BRASIL. Artigos 138, 139 e 140 do CP, **Decreto Lei 2.848 de 07 de dezembro de 1940.**

BRASIL. Artigos 240, 241, 241-A, 241-B, 241-C, 241-D, 241-E do ECA, **Lei 8.089**, de 13 de julho de 1990.

BRASIL. Artigos 67 e 68 do CP, **Decreto Lei 2.848 de 07 de dezembro de 1940.**

BRASIL. Consolidação das Leis do Trabalho (CLT). **Decreto-Lei nº 5.452, de 1º de maio de 1943**. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del5452.htm.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Atualizada pela EC 115/2022.

BRASIL. Constituição de 1988. **Constituição da República Federativa do Brasil de 1988**. Brasília: Presidência da República, 2022. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.html. Acesso em: 25 mai.2025.

BRASIL. Lei Geral de Proteção de Dados Pessoais (LGPD), **Lei nº 13.709/2018**.

BRASIL. **Parecer Às Emendas De Plenário Ao Projeto De Lei nº 21, De 2020**. Brasília: Câmara dos Deputados, 2021. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=node0pc68bsnubpp9bylht3gvtel668608.node0?codteor=2082277&filename=Parecer-CCTCI-29-09-2021. Acesso em: 21 maio. 2022.

BRASIL. Tribunal Superior do Trabalho. **Recurso de Revista n. 0010236-94.2022.5.03.0013**. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/tst/1939429194>.

CANALES, Katie. **China's 'social credit' system ranks citizens and punishes them with throttled internet speeds and flight bans if the Communist Party deems them untrustworthy**. Business Insider, 24/12/2021. Disponível em: <https://www.businessinsider.com/china-social-credit-system-punishments-and-rewards-explained-2018-4>. Acesso em: 29 maio. 2022.

CELLAN-JONES, Rory. **Stephen Hawking warns artificial intelligence could end mankind**. Disponível em: <https://www.bbc.com/news/technology-30290540>. Acesso em: 21 mai. 2025.

CHAI, Cassius Guimaraes; LIMA, Pedro H. Roque. **A.I. Entre Privacidade Vs. Danos E Riscos À Saúde Pública: Uso De Dados Randomizados Da Telefonia Móvel Como Estratégia De Prevenção E Proteção Da Saúde Pública No Combate Ao Covid-19**. Skema Business School, Belo Horizonte/MG, 2020. Disponível em: <http://site.conpedi.org.br/publicacoes/x2c7701f/q496y020/xGUox6fW6qJ5RLIH.pdf>. Acesso em: : 21 maio. 2025.

CHAVES JUNIOR, Airto; BERZAGUI, Bruno. Máquinas autônomas e responsabilidade no âmbito do direito penal: uma análise a partir da teoria da ação significativa. **Revista Eletrônica Direito e Política, Programa de Pós-Graduação Stricto Sensu em Ciência Jurídica da UNIVALI, Itajaí**, v.16, n.3, 3º quadrimestre de 2021. Disponível em: www.univali.br/direitoepolitica - ISSN 1980-7791. Acesso em: : 21 maio. 2025.

DE ANDRADE, Fabio Siebeneichler; FACCIO, Lucas Girardello. **Notas sobre a responsabilidade civil pela utilização da inteligência artificial**. Doutrina Nacional, v. 46, n. 146, p. 153, 2019.

DE FERNANDES TEIXEIRA, João. **O cérebro e o robô: inteligência artificial, biotecnologia e a nova ética**. Pia Sociedade de São Paulo-Editora Paulus, 2016.

DE STEFANO, Valerio. The rise of the “just-in-time workforce”: **On-demand work, crowdwork and labor protection in the “gig-economy”**. Geneva: ILO, 2016.

DE TEFFÉ, Chiara Spadaccini; MEDON, Filipe. **Responsabilidade civil e regulação de novas tecnologias**: questões acerca da utilização de inteligência artificial na tomada de decisões empresariais. REI, v. 6, n. 1, p. 301-333, 2020.

DE TEFFÉ, Chiara Spadaccini; VIOLA, Mario. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais. **Civilistica.com**, v. 9, n. 1, p. 1-38, 2020.

DELGADO, Mauricio Godinho. **Curso de Direito do Trabalho**. 20. ed. São Paulo: LTr, 2020.

DURAND, Cédric. Tecnofeudalismo: **crítica da economia digital**. São Paulo: Autonomia Literária, 2021.

FONSECA, Aline Klayse. Delineamentos jurídico-dogmáticos da inteligência artificial e seus impactos no instituto da responsabilidade civil. **Civilistica.com**, v. 10, n. 2, p. 1-36, 2021.

FORNASIER, Mateus de Oliveira; BECK, Cesar. **CAMBRIDGE ANALYTICA: ESCÂNDALO, LEGADO E POSSÍVEIS FUTUROS PARA A DEMOCRACIA**. Revista Direito Em Debate, 29(53), 182-195, 2020.

GARCIA, Lara Rocha et al. **Lei Geral de Proteção de Dados (LGPD): Guia de implantação**. Editora Blucher, 2020.

GOLDSCHMIDT, Rodrigo; CANI, Elcemara Aparecida Zielinski. Relações entre trabalhadores e plataformas e aplicativos: da ausência de subordinação à subordinação algorítmica. **Revista do TRT da 12ª Região**, v. 25, n. 34, p. 151-170, 2022.

GOOD, I. J. **Speculations Concerning the First Ultraintelligent Machine**. Advances in Computers, volume 6, 1965. Página 31.

GOULART, Guilherme Damásio. **O impacto das novas tecnologias nos direitos humanos e fundamentais: o acesso à internet e a liberdade de expressão**. REDESG, Universidade Federal de Santa Maria. Santa Maria/RS, 2012.

GOVERNO DA REPÚBLICA POPULAR DA CHINA. 社会信用体系建设规划纲要 (2014—2020年) (*Esquema do Planejamento de Construção do Sistema de Crédito Social (2014-2020)*). 27/06/2014. Disponível em: <http://www.gov.cn/zhengce/content/2014-06/27/content_8913.htm>. Acesso em: 21 maio. 2025.

KEARNS, Michael; ROTH, Aaron. **The Ethical Algorithm**. Oxford University Press, 2020.

KIRCHNER, Isabel Luiza. **O uso da Inteligência Artificial sob a ótica dos direitos fundamentais: análise do caso Amazon**. Trabalho de Conclusão de Curso. Universidade Federal do Rio Grande do Sul (2020).

KOBS, Anderson Vagner; VIEIRA, Sylvio André Garcia. Cibersegurança: identificação de Keystroke por dispositivo Rubber Ducky. **Disciplinarum Scientia**, v. 22, n. 1, p. 135-149, 2021.

LAVADO, T. **Aumento do uso de reconhecimento facial pelo poder público no Brasil levanta debate sobre limites da tecnologia**. G1, Economia, Tecnologia, 21/02/2020. Disponível em: <<https://g1.globo.com/economia/tecnologia/noticia/2020/02/21/aumento-do-uso-de-reconhecimento-facial-pelo-poder-publico-no-brasil-levanta-debate-sobre-limites-da-tecnologia.ghtml>>. Acesso em: 04 jun. 2025.

LEE, Kai-Fu. **Inteligência artificial: Como os robôs estão mudando o mundo, a forma como amamos, nos relacionamos, trabalhamos e vivemos**. Globo Livros, 2019.

MARQUES, C. L.; BENJAMIN, A. H.; MIRAGEM, B. Comentários ao código de defesa do consumidor. **Revista dos tribunais**, 2013.

MPT - Ministério Público do Trabalho. **Nota Técnica sobre trabalho por plataformas digitais**. Brasília: 2021.

MPT - Ministério Público do Trabalho. **O uso de dados pessoais e inteligência artificial na relação de trabalho**. Brasília: 2022.

PANTOJA, Adilson Carvalho; LEÃO, Semírames de Cássia **Lopes. Inteligência Artificial e Justiça do Trabalho: desafios atuais**. In: MPT, 2022.

PARLAMENTO EUROPEU. **Resolução do Parlamento Europeu, de 16 de fevereiro de 2017**, Disposições de Direito Civil sobre Robótica (2015/2103(INL)). Disponível em: <https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_PT.html>. Acesso em: 21 mai. 2025.

PINHEIRO, Patrícia Peck. **Proteção de Dados Pessoais: Comentários à Lei n. 13.709/2018-LGPD**. Saraiva, 2020.

PRASSL, Jeremias. **Humans as a Service: The Promise and Perils of Work in the Gig Economy**. Oxford: OUP, 2017.

RAPÔSO, Cláudio Filipe Lima et al. **LGPD – Lei geral de proteção de dados pessoais em tecnologia da informação: Revisão sistemática**. RACE, v. 4, p. 58-67, 2019.

RAPÔSO, Cláudio Filipe Lima et al. LGPD-lei geral de proteção de dados pessoais em tecnologia da informação: Revisão sistemática. **RACE-Revista de Administração do Cesmac**, v. 4, p. 58-67, 2019.

Report to the Mayor of London. Disponível em:

<https://www.london.gov.uk/sites/default/files/040910_letter_to_unmesh_desai_am_report_re_kings_cross_data_sharing.pdf>. Acesso em: 03 jul.2025.

RODRIGUES, Rosemberg Augusto Pereira. **Proteção de dados pessoais como um direito fundamental: o que muda em sua vida com a inclusão dessa garantia na Constituição Federal?** SERPRO, 2022. Disponível em: <<https://www.serpro.gov.br/menu/noticias/noticias-2022/protecao-de-dados-pessoais-como-um-direito-fundamental>>. Acesso em: 04 jul. 2025.

SABBAGH, D. **Facial recognition row: police gave King's Cross owner images of seven people**. The Guardian, Technology, 04/10/2019. Disponível em: <<https://www.theguardian.com/technology/2019/oct/04/facial-recognition-row-police-gave-kings-cross-owner-images-seven-people>>. Acesso em: 21 mai. 2025.

SANTOS, Arnaldo Gonçalves Dias. **A responsabilidade civil dos danos causados por inteligência artificial**. Revista Jus Navigandi, 2020. Disponível em: <<https://jus.com.br/artigos/84834/a-responsabilidade-civil-dos-danos-causados-por-inteligencia-artificial>>. Acesso em: 21 maio. 2025.

SCHWAB, Klaus. **A Quarta Revolução Industrial**. São Paulo: Edipro, 2016.

SILVA, Rodrigo de Bona. **Sociedade e Estado: Quem Controla Quem?** Diferentes abordagens do controle social e a evolução das relações Sociedade-Estado. Revista da CGU, v. 8, n. 13, p. 404-423, 2016.

TEFFÉ, Chiara Spadaccini de; VIOLA, Mario. **Tratamento de dados pessoais na LGPD: estudo sobre as bases legais**. Civilistica.com. Rio de Janeiro, a. 9, n. 1, 2020. Disponível em: <<http://civilistica.com/tratamento-de-dados-pessoais-na-lgpd/>>.

TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO. **Recurso Ordinário Trabalhista (ROT) n. 1001005-80.2023.5.02.0025**. Relatora: Ivani Contini Bramante. 4ª Turma, Cadeira 5, julgado em 15 maio 2024. Disponível em: <https://trt2.jus.br>. Acesso em: 24 maio 2026.

VECTRA Consultoria e Serviços. **Conheça os 6 principais tipos de crime na internet.** Disponível em: <https://blog.vetracs.com.br/conheca-os-6-principais-tipos-de-crime-na-internet/>.

ZUBOFF, Shoshana. **A era do capitalismo de vigilância:** a luta por um futuro humano na nova fronteira do poder. Rio de Janeiro: Intrínseca, 2020.

ZUBOFF, Shoshana. **A Era do Capitalismo de Vigilância:** A luta por um futuro humano na nova fronteira de poder. Editora Intrínseca, 2019.