OS IMPACTOS DO USO DA INTELIGÊNCIA ARTIFICIAL NO MONITORAMENTO INTELIGENTE DE FUNCIONÁRIOS E COMPARTILHAMENTO INDEVIDO DE DADOS: UM ESTUDO DE CASO

Autores: Carolina dos Santos Pereira[1], Raica Gonçalves Gramacho[2], Viviane Paula dos Santos Jesus[3].

Escola Máximu's/Instituto Ribeiro Goulart,R. Isac Newton, 37 - Jardim Oriental, São José dos Campos - SP, 12236-240, Brasil, carolinadossantospereira78@gmail.com, raica.goncalves209@gmail.com, vivianepaulad@gmail.com

Resumo
O uso de monitoramento digital está cada vez mais presente nas empresas no cenário atual. Com o avanço da tecnologia e o crescimento do trabalho remoto e híbrido, mais da metade das organizações passaram a usar ferramentas digitais para acompanhar as atividades dos funcionários. O presente trabalho tem como foco o estudo do uso da Inteligência Artificial no monitoramento de funcionários dentro do ambiente corporativo. A pesquisa busca compreender como o sistema de IA opera na coleta, armazenamento e análise de dados, bem como impactos jurídicos, sociais e éticos dessa prática. Através de uma revisão bibliográfica quantitativa e qualitativa concluiu-se que o controle e o monitoramento de funcionários são necessários para manter o bom funcionamento e progresso da empresa bem como a garantia e preservação dos direitos dos funcionários.

Palavras-chave: Inteligência Artificial. Local de Trabalho. Monitoramento digital. Privacidade.

Área do Conhecimento: Ensino Médio/Técnico

Introdução

Marcado pelo avanço acelerado da tecnologia e da digitalização em todos os setores da atualidade, percebe-se que o ambiente de trabalho não é exceção. Com esse vertiginoso avanço da tecnologia as empresas possuem a total permissão da utilização de monitoramento digital para acompanhar as atividades dos funcionários no trabalho (Struzano, 2024). Embora possa aumentar a eficiência e segurança, também levanta questões éticas e legais como, desvio de finalidade, coleta excessiva de dados, falta de transparência, discriminação, danos a integridade psíquica e viola ao direito à privacidade do trabalhador. Nesse contexto, este trabalho tem o intuito de avaliar o funcionamento da Inteligência Artificial (IA) no monitoramento inteligente de funcionários, analisando como ocorre a coleta e a análise de dados, identificando possíveis violações de direitos, suas causas, e o limite do controle tecnológico nas empresas. Através de uma revisão bibliográfica quantitativa e qualitativa concluiu-se que o controle e o monitoramento de funcionários são necessários.

Metodologia

A metodologia adotada neste trabalho foi de natureza quantitativa e qualitativa que é definida como aquela que privilegia a análise de micro processos, através do estudo das ações sociais individuais e grupais, realizando um exame intensivo dos dados, e caracterizada pela heterodoxia no momento da análise (Martins, 2004). Dentro desta metodologia foi adotado uma Pesquisa Documental e Análise de dados secundários que representam a estratégia eficaz quando se colocam questões "como'' e "por que'', quando o pesquisador tem pouco controle sobre os eventos e quando o foco se encontra em fenômenos contemporâneos inseridos em algum contexto da vida real (Yin, 2004). Para isso estruturam-se em duas etapas principais.

Na primeira etapa realizou-se uma revisão bibliográfica apresentando uma visão geral sobre o que é inteligência artificial e conceitos com o objetivo de familiarizar-se com a temática, mostrando que a IA tem desempenhado um papel crucial na transformação de empresas.

Na segunda foi abordado o tema sobre questões éticas, focando na segurança dos dados pessoais dos funcionários, sua privacidade e monitoramento dentro da empresa. Foi discutida também a

importância dos processos de produção, gerenciamento de riscos e gestão através do estudo de caso, analisando o artigo referente para melhor compreensão do assunto.

Resultados

Os dados obtidos durante a pesquisa foram submetidos à análise qualitativa, permitindo a identificação de categorias interpretativas relevantes para o alcance dos objetivos propostos neste estudo.

Foi identificado que empresas que adotam softwares de monitoramento profissional estão permitindo o compartilhamento de informações pessoais e hábitos digitais de funcionários com grandes companhias de tecnologia e publicidade. A conclusão aparece em uma pesquisa divulgada recentemente por pesquisadores da *Northeastern University*, nos Estados Unidos. O relatório aponta que o compartilhamento de dados ocorre de maneira opaca, contínua e, frequentemente, sem que o trabalhador tenha conhecimento ou capacidade de escolha.

A pesquisa aponta que os dados são vazados através de plataformas de monitoramento intermediárias que transmitem os dados de identificação dos funcionários e suas atividades para redes de anúncios, empresas de tecnologia e corretores de dados, apontando que o compartilhamento de dados quando os funcionários acessam essas plataformas por navegadores web é maior do que quando utilizam aplicativos móveis específicos e que muitas vezes, esses dados são integrados a perfis comportamentais maiores de consumidores através de ferramentas de rastreamento comerciais integradas por padrão (*default-on*) dentro do código do software.

Além de sua utilização para fins comerciais, especialmente no mercado publicitário, os dados coletados a partir das atividades e da produtividade dos trabalhadores podem ser compartilhados e utilizados pelas empresas responsáveis pelos sistemas de monitoramento para o treinamento e aperfeiçoamento de modelos de inteligência artificial, tanto próprios quanto desenvolvidos por terceiros.

Tabela 1 – Apresentação dos Resultados

Empresa	Trabalhador	Nº de ocorrências de compartilhamento de informações	Tipos de dados relacionados ao trabalhador compartilhados com terceiros	Empresa terceira (para onde os dados foram enviados)
Apploye	Gerente	3	E-mail, nome	Facebook (e-mail); Promptwatch (nome, e-mail)
Apploye	Não gerente	1	E-mail	Facebook (e-mail)
Buddy Punch	Gerente	9	E-mail, nome, nome da empresa	Warmly (nome, e-mail); Facebook (e-mail); Intercom (nome, e-mail, nome da empresa); Wootric (e-mail); ReferralHero (nome, e-mail)
Buddy Punch	Não gerente	2	E-mail	Facebook (e-mail); Wootric (e-mail)
Deputy	Gerente	8	E-mail, nome, sobrenome, nome da empresa	Amazon CloudFront (nome da empresa); Segment (nome da empresa, nome, sobrenome, e-mail); WalkMe (e-mail, nome da empresa); Datadog (nome da empresa)
Deputy	Não gerente	5	E-mail, nome, sobrenome, nome da empresa	Segment (nome, sobrenome, e-mail, nome da empresa); Amazon CloudFront (nome da empresa)
Desklog	Gerente	2	E-mail	Functional Software (e-mail); Facebook (e-mail)
Desklog	Não gerente	1	E-mail	Functional Software (e-mail)
Hubstaff	Gerente	15	E-mail, nome, sobrenome, nome da empresa	Segment (nome, sobrenome, e-mail, nome da empresa); Google APIs (nome, sobrenome, e-mail, nome da empresa); ProfitWell (e-mail); Facebook (e-mail, nome, sobrenome); HubSpot (nome, sobrenome, e-mail)
Hubstaff	Não gerente	14	E-mail, nome, sobrenome, nome da empresa	Segment (nome, sobrenome, e-mail, nome da empresa); Google APIs (nome, sobrenome, e-mail, nome da empresa); ZoomInfo (e-mail, nome da empresa); Facebook (e-mail, nome da empresa); ProfitWell (e-mail); HubSpot (e-mail)
Monitask	Gerente	6	E-mail, nome, sobrenome	Microsoft (e-mail); ProfitWell (e-mail); SatisMeter (e-mail); Intercom (e-mail, nome, sobrenome)
Monitask	Não gerente	5	E-mail	Microsoft (e-mail); Intercom (e-mail); Dreamdata (e-mail); SatisMeter (e-mail); ProfitWell (e-mail)
Time Doctor	Gerente	16	E-mail, nome, sobrenome	Segment (e-mail, nome, sobrenome); Facebook (e-mail, nome, sobrenome); Dreamdata (e-mail); Functional Software (e-mail, nome, sobrenome); Amplitude (nome, sobrenome, e-mail); Ahrefs (nome, sobrenome); ProfitWell (e-mail)
Time Doctor	Não gerente	6	E-mail, nome, sobrenome	Segment (e-mail, nome, sobrenome); ProfitWell (e-mail); Amplitude (e-mail); HubSpot (e-mail)

Fonte Adaptada: “Plataformas de monitoramento no local de trabalho estão compartilhando seus dados: uma investigação e um roteiro para combater o abuso de dados.” *Columbia Law School*, 2026.

Discussão

A análise dos dados revelados pela investigação "*Workplace Monitoring Platforms Are Sharing Your Data*" (2026) oferece uma base factual crítica para compreender os impactos reais da Inteligência Artificial (IA) no monitoramento inteligente de funcionários. Os achados demonstram que a convergência entre ferramentas de vigilância laboral (*boxware*) e algoritmos de IA transformou a

supervisão de uma atividade de conformidade local para um ecossistema complexo de extração de valor e controle preditivo.

O primeiro grande impacto da IA no monitoramento inteligente refere-se à mudança na natureza do dado coletado. Antes da popularização da IA, o monitoramento buscava apenas flagrar infrações ou medir horas trabalhadas. Hoje, os achados da pesquisa evidenciam esse ciclo: dados de cliques (*keystrokes*), movimentos de mouse, páginas visitadas e rotinas diárias dos funcionários de plataformas como *Hubstaff* e *Time Doctor* 2 estão sendo ativamente repassados para treinar modelos de inteligência artificial de terceiros.

A introdução de IA no monitoramento expande a vigilância para a esfera física e comportamental através de sensores. A revelação de que três das nove plataformas analisadas exigem acesso aos sensores físicos do smartphone (acelerômetro e giroscópio) para validar o *clock-in* exemplifica como a IA é utilizada. Os sistemas inteligentes não buscam apenas saber se o funcionário está logado, mas analisam, por meio desses sensores e de algoritmos de aprendizado de máquina, os padrões físicos de movimento para deduzir estados de atenção, cansaço ou ócio. Essa análise algorítmica retira o fator humano da avaliação de desempenho: a máquina passa a ditar o ritmo ideal de trabalho com base em médias matemáticas frias, ignorando as nuances biológicas e psicológicas do ser humano, o que agrava os riscos de adoecimento mental e *Burnout*.

Por fim, as menções do artigo a órgãos reguladores (como a FTC e o CFPB) e a casos de grandes empresas (como a *xAI* exigindo a instalação compulsória de softwares de monitoramento) expõem como os sistemas de monitoramento inteligente frequentemente operam sob a lógica da "caixa-preta" (*black box*), onde os critérios utilizados pelos algoritmos para classificar um funcionário como "produtivo" ou "improdutivo" são opacos e inacessíveis. Quando esses dados vazam e são mercantilizados de forma contínua por ferramentas *default-on*, o trabalhador perde o controle sobre sua própria reputação profissional. Se um perfil comportamental negativo for gerado por uma IA e compartilhado com data *brokers*, esse indivíduo pode ser silenciosamente penalizado em processos seletivos futuros em outras empresas, sem nunca saber o real motivo de sua exclusão.

Os resultados apresentados por Nguyen et al. (2026) demonstram que as tecnologias de monitoramento digital de funcionários estão ultrapassando a simples função de acompanhamento da produtividade e assumindo características de um sistema abrangente de vigilância de dados. A pesquisa revelou que todas as nove plataformas analisadas compartilharam informações pessoais dos trabalhadores com empresas terceiras, incluindo: nome, sobrenome, e-mail e nome da organização empregadora. Ao todo, foram identificadas 121 ocorrências de compartilhamento de dados pessoais e 145 domínios de terceiros que receberam informações relacionadas às atividades online dos funcionários.

Esses resultados evidenciam um cenário preocupante quando associado ao avanço da Inteligência Artificial (IA). Os dados coletados pelas plataformas de monitoramento constituem uma matéria-prima valiosa para sistemas de IA, que dependem de grandes volumes de informações para treinamento e aprimoramento de algoritmos. O próprio estudo destaca que os dados dos trabalhadores podem ser utilizados para treinar modelos de inteligência artificial cujos usos futuros podem ser prejudiciais aos próprios funcionários monitorados.

Conclusão

O impacto do monitoramento digital de funcionários, potencializado pela Inteligência Artificial e pelo compartilhamento indevido de dados, representa uma das transformações mais profundas e alarmantes nas relações de trabalho contemporâneas. A análise desse cenário revela que a vigilância laboral deixou de ser uma ferramenta de gestão de conformidade para se tornar um sistema de extrativismo de dados e controle biopsicossocial.

O monitoramento inteligente sem limites éticos ou jurídicos estabelece uma assimetria de poder sem precedentes entre empregador e empregado. O direito à privacidade e a dignidade humana não podem ser mitigados em nome da eficiência empresarial.

Diante desse cenário, é essencial que as empresas adotem medidas que garantam a conformidade com a legislação de proteção de dados, como a Lei Geral de Proteção de Dados (LGPD), além de promover transparência sobre os métodos de monitoramento utilizados. Portanto, o desafio não está apenas na implementação da inteligência artificial, mas em assegurar que sua aplicação respeite os direitos dos trabalhadores, conciliando inovação tecnológica, produtividade e proteção da privacidade. Dessa forma, será possível construir ambientes de trabalho mais éticos, seguros e alinhados às exigências da sociedade digital contemporânea.

A revisão bibliográfica permitiu criar uma visão ampla sobre o uso da inteligência artificial para monitoramento de funcionários mostrando sua importância em garantir o cumprimento da LGPD e evitar prejuízos a empresa e garantir o bem estar do funcionário.

Referências

GONÇALVES, Aline Menezes; MARTINS, Gabriel Henrique Struzano;, Guilherme Torres. O DIREITO À PRIVACIDADE DO TRABALHADOR EM TEMPOS DE MONITORAMENTO DIGITAL NO LOCAL DE TRABALHO. In: **ANAIS DO CONGRESSO INTERNACIONAL DE DIREITOS HUMANOS E NOVOS PARADIGMAS**. 2024. p. e006-e006.

Levi Kaplan and Stephanie T. Nguyen, David Choffnes, Alan Mislove, Seth Frotman, Erie Meyer, Workplace Monitoring Platforms Are Sharing Your Data: An Investigation & Roadmap to Address Data Abuses, (2026). Available at: https://scholarship.law.columbia.edu/law_economy/5

MARTINS, Heloisa Helena T. Metodologia qualitativa de pesquisa. **Educação e pesquisa**, v. 30, n. 02, p. 289-300, 2004.

YIN, Robert K. **The case study anthology**. Sage, 2004.