Lex Publica
Jurnal Ilmu Hukum Asosiasi Pimpinan Perguruan Tinggi Hukum Indonesia
e-ISSN: 2579-8855
p-ISSN: 2354-9181
https://journal.appthi.org/index.php/lexpublica

Ethical and Legal Concerns of Artificial Intelligence in the Workplace: Examining Current Legislations in the United States

Tri Rudiyanto[1*], Halley Kunda[1], Amy Dunn[1], Sharon Shenderovskiy[1], and Rondarrius Gibson[1]

[1] Warrington College of Business, University of Florida, Gainesville, United States

**Corresponding author: tri.rudiyan@ufl.edu*

Abstract. The emergence of remote work prompted by the global Covid-19 pandemic has transformed workplace dynamics, highlighting intricate concerns about employee privacy and autonomy. However, the rise of algorithmic management driven by artificial intelligence (AI) challenges the assumed privacy in remote work settings. This paper examines the ethical and legal landscape of AI-powered employee monitoring in the United States. It employs a mixed-methods approach, incorporating literature review, case analysis, legal examination, and ethical analysis. Past cases reveal the complex interaction between personal privacy and employer surveillance, offering insights for current and future legal actions. Current legislation, including the Electronic Communications Privacy Act (ECPA), is explored, along with state-specific laws and their implications. Ethical concerns encompass biometric data tracking, discriminatory biases, and gig economy surveillance. AI's impact on employee behavior and future implications are discussed, suggesting the need for balanced policies that prioritize transparency, fairness, accountability, and trust. In navigating the challenges of AI-powered monitoring, organizations should consider ethical considerations, existing legislation, and future trends to create a harmonious work environment that respects individual rights.

Keywords: Algorithmic management, AI-powered employee monitoring, Privacy, Legality, Ethical concerns

Abstrak. *Munculnya kerja jarak jauh yang dipicu oleh pandemi global Covid-19 telah mengubah dinamika tempat kerja, menyoroti keprihatinan rumit tentang privasi dan otonomi karyawan. Namun, munculnya manajemen berbasis algoritma yang digerakkan oleh kecerdasan buatan (AI) menantang privasi yang diasumsikan dalam pengaturan kerja jarak jauh. Makalah ini mengkaji lanskap etika dan hukum dari pemantauan karyawan yang didukung oleh AI di Amerika Serikat. Ini menggunakan pendekatan metode campuran, menggabungkan tinjauan pustaka, analisis kasus, pemeriksaan hukum, dan analisis etika. Kasus-kasus masa lalu mengungkapkan interaksi kompleks antara privasi pribadi dan pengawasan oleh pemberi kerja, memberikan wawasan untuk tindakan hukum saat ini dan masa depan. Undang-undang saat ini, termasuk Undang-Undang Privasi Komunikasi Elektronik (ECPA), dieksplorasi, bersama dengan undang-undang khusus negara dan implikasinya. Keprihatinan etika meliputi pelacakan data biometrik, bias diskriminatif, dan pengawasan ekonomi tumpahan. Dampak AI pada perilaku karyawan dan implikasi masa depan dibahas, menunjukkan perlunya kebijakan yang seimbang yang mengutamakan transparansi, keadilan, akuntabilitas, dan kepercayaan. Saat mengatasi tantangan pemantauan yang didukung oleh AI, organisasi harus mempertimbangkan pertimbangan etika, undang-undang yang ada, dan tren masa depan untuk menciptakan lingkungan kerja yang harmonis yang menghormati hak individu.*

Kata kunci: *Manajemen algoritmik, Pemantauan karyawan yang didukung AI, Privasi, Legalitas, Masalah etika*

Lex Publica
Vol. 10, No. 1, 2023, 84-100

1. Introduction

The contemporary landscape of workplaces has experienced a seismic and transformative shift, catalyzed by the widespread adoption of remote work—a paradigm that has gained unprecedented momentum, driven by the global Covid-19 pandemic.[1] This monumental shift in work dynamics has not only reconfigured the tangible aspects of physical workspaces but has also brought to the forefront a complex interplay of issues concerning employee privacy and autonomy.[2] Contrary to initial assumptions that remote work would inherently afford employees greater privacy within their own spaces, a closer and more discerning examination reveals a multifaceted and nuanced reality, significantly shaped by the pervasive rise of algorithmic management—an augmentation facilitated by the dynamic integration of artificial intelligence (AI) into organizational practices.[3]

In the context of remote work environments, this trend towards algorithmic management has ignited a symphony of ethical and legal debates, particularly in the United States, that underscore the intrinsic tension between the pursuit of optimized corporate productivity through surveillance mechanisms and the preservation of individuals' fundamental rights.[4] This intricate balance, or rather imbalance, brings to the forefront pressing questions that delve deep into the heart of modern workplace dynamics.[5]

Corporations and enterprises have embarked on a trajectory of progressively embracing sophisticated technological tools to monitor and manage their remote workforce.[6] The spectrum of surveillance mechanisms employed in this context is vast, encompassing a wide range of strategies that traverse the continuum from subtle and almost imperceptible website tracking to more invasive and intimate interventions such as keystroke monitoring and the activation of computer web

[1] Mohammad Faraz Naim, "Revamping workplace learning and development during Covid-19 in HR consulting industry in India: a thematic analysis," *International Journal of Knowledge and Learning* 16, no. 3 (2023): 274.

[2] Stephen Blumenfeld, Gordon Anderson, and Val Hooper, "Covid-19 and employee surveillance," *New Zealand Journal of Employment Relations* 45, no. 2 (2020): 50.

[3] Tomas Chamorro-Premuzic, "Can surveillance AI make the workplace safe?," *MIT Sloan Management Review* 62, no. 1 (2020): 13.

[4] Fairweather, N. Ben, "Surveillance in employment: The case of teleworking," in *Computer Ethics*, ed. John Weckert, (London: Routledge, 2017), 390.

[5] Banu Saatçi, Roman Rädle, Sean Rintel, Kenton O'Hara, and Clemens Nylandsted Klokmose, "Hybrid meetings in the modern workplace: stories of success and failure," in *Collaboration Technologies and Social Computing: 25th International Conference,* CRIWG+ CollabTech 2019, Kyoto, Japan, September 4–6, 2019, Proceedings 25 (Springer International Publishing, 2019), 45.

[6] Christina S. Hagen et al., "Why are you watching? Video surveillance in organizations," *Corporate Communications: An International Journal* 23, no. 2 (2018): 274.

cameras. This technological progression, heralded by its proponents as a means to achieve efficiency and a heightened sense of accountability, has inadvertently triggered an extensive discourse that not only revisits historical instances of privacy violations but also contemplates the intricacies of the contemporary legal framework that governs these practices, not to mention the ever-evolving ethical implications embedded within today's dynamic professional landscape.[7]

By delving into the annals of history and scrutinizing past cases where employee monitoring has encroached upon personal privacy, an undeniable pattern emerges—one that elucidates that the current accelerated adoption of algorithmic management is not a novel challenge.[8] Historical records are replete with instances of unwarranted incursions into employees' digital sanctums, serving as poignant cautionary tales that echo through the digital corridors of today's interconnected and digitally driven workplaces.[9] These historical illustrations collectively underscore an unequivocal need: the imperative to strike a harmonious equilibrium between the strategic objectives of corporations and the inherent and sacrosanct rights of individuals—rights that pertain to autonomy, dignity, and an indispensable sphere of personal privacy.[10]

Amid this intricate backdrop, the United States grapples with the evolving nature of employee surveillance through the intricate tapestry of legislation—a patchwork that aims to address the swiftly transforming landscape of work, powered by algorithmic management and AI-driven monitoring.[11] However, these legislative endeavors often grapple with the challenge of keeping stride with the breakneck pace of technological evolution.[12] Hence, a comprehensive exploration of these prevailing legislations, along with their implications and inevitable

[7] Gundars Kaupins and Malcolm Coco, "Perceptions of internet-of-things surveillance by human resource managers," *SAM Advanced Management Journal* 82, no. 2 (2017): 53. See also, Ingrid Nappi and Gisele de Campos Ribeiro, "Internet of Things technology applications in the workplace environment: A critical review," *Journal of Corporate Real Estate* 22, no. 1 (2020): 80.

[8] Ifeoma Ajunwa, Kate Crawford, and Jason Schultz, "Limitless worker surveillance," *California Law Review* 105, no. 3 (2017): 735.

[9] Antonio Aloisi and Valerio De Stefano, "Essential jobs, remote work and digital surveillance: Addressing the Covid-19 pandemic panopticon," *International Labour Review* 161, no. 2 (2022): 291.

[10] Charles P. Nemeth, *Private security and the law* (Boca Raton: CRC Press, 2017), 23. See also, Mark Button and Peter Stiernstedt, "Comparing private security regulation in the European Union," In *The Rise of Comparative Policing*, ed. Jacques de Maillard and Sebastian Roché (London: Routledge, 2021), 36.

[11] Kathryn Zickuhr, "Workplace surveillance is becoming the new normal for US workers," *Washington Center for Equitable Growth*, August 17, 2021, https://equitablegrowth.org/research-paper/workplace-surveillance-is-becoming-the-new-normal-for-u-s-workers/.

[12] Mahmoud Moussa, "Monitoring employee behavior through the use of technology and issues of employee privacy in America," *Sage Open* 5, no. 2 (2015): 3. See also, Devasheesh P. Bhave, Laurel H. Teo, and Reeshad S. Dalal, "Privacy at work: A review and a research agenda for a contested terrain," *Journal of Management* 46, no. 1 (2020): 130.

limitations, becomes an essential endeavor—one that is crucial in grasping the full scope of the current legal landscape surrounding the marriage of algorithmic management and AI-powered employee monitoring.

As we embark on a contemplative journey, navigating through the multifaceted implications of algorithmic management and its synergistic interplay with AI-driven monitoring in the profound reshaping of the contours of work, a medley of ethical concerns emerges as a critical theme. These concerns transcend the mere realm of legal compliance and enter the ethereal territory of profound ethical intricacies. The ethical landscape unfurls, enfolding themes of consent, autonomy, fairness, and the potential erosion of the psychological compact between employers and employees—a compact that has for centuries underpinned the foundational relationship within workplaces. These ethical considerations assume a pivotal role in shaping the trajectory of future work dynamics, demanding a meticulous exploration of the tensions that inevitably arise between the imperatives of relentless innovation and the immutable imperative of embedding human-centric values and practices within the modern workplace paradigm.

2. Methods

This research employs a descriptive and qualitative approach encompassing literature review, case analysis, legal examination, and ethical analysis. The literature review provides a foundation by identifying key themes in algorithmic management, AI-driven employee monitoring, workplace ethics, and legal frameworks. Case analysis involves purposive selection of diverse instances of employee monitoring to uncover specific ethical and legal challenges. Legal analysis involves scrutinizing relevant United States legislations such as the Electronic Communications Privacy Act (ECPA) and the National Labor Relations Act (NLRA) to discern their applicability and limitations. Ethical analysis employs a framework encompassing consent, autonomy, fairness, and transparency to evaluate the moral implications. Integrating these findings offers a comprehensive understanding of the multifaceted ethical and legal landscape surrounding algorithmic management and AI-driven monitoring in the workplace.

3. Results and Discussion

3.1. Understanding Past Cases

Studying past cases offers invaluable insights for determining the appropriate handling and resolution of present ethical dilemmas.[13] By examining a range of cases, including notable instances such as Stengart v. Loving Care Agency, Pure Power Boot Camp, Inc. v. Warrior Fitness Boot Camp, LLC, and Jennings vs. Jennings, the court gains a wellspring of insights, enabling the drawing of pertinent precedents that can illuminate the way these types of cases should be addressed.

In the Stengart v. Loving Care Agency case, the central figures were Loving Care, the employer, and Marina Stengart, an employee.[14] In 2010, Stengart utilized her work computer to communicate with her personal attorney, discussing her adverse work conditions and potential litigation. Following her resignation and the return of the computer, Loving Care enlisted a technology expert to recover Stengart's emails to her attorney from the hard drive. These emails were subsequently used by Loving Care in the legal proceedings initiated by Stengart. The court ruled that Stengart was aware that the emails on the computer were Loving Care's property, thus rejecting her request to disqualify them. After an appeal by Stengart, the appellate court determined that Loving Care had violated N.J. R. Prof. Conduct 4.4(b), prompting further review by the New Jersey Supreme Court. The pivotal concern in this case revolved around whether an employee could reasonably expect privacy protection for a personal, password-protected, web-based email account accessed via an employer's computer. Ultimately, the Supreme Court of New Jersey ruled affirmatively, emphasizing that Stengart's personal email account retained protection even when accessed on a computer owned by Loving Care.[15]

Shifting focus to the Pure Power Boot Camp, Inc. v. Warrior Fitness Boot Camp, LLC case of 2010, the scenario involved employer access to employee emails, yielding a distinct outcome.[16] Lauren Brenner, the owner of Pure Power Boot Camp (PPBC), employed Reuben Belliard and Alex Fell, ex-Marines, as drill instructors (Pure Power Boot Camp, inc. v. warrior fitness Boot Camp, LLC - 759 F. supp. 2d 417. Following Belliard's departure and Fell's termination, they launched Warrior Fitness Boot Camp (WFBC) with their girlfriends, Jennifer Lee

[13] Odies C. Ferrel and John Fraedrich, *Business ethics: Ethical decision making and cases* (Canada: Cengage learning, 2021), 25.

[14] Stengart v. Loving Care Agency, Inc., 201 N.J. 300, 990 A.2d 650 (N.J. 2010). Retrieved January 26, 2023, https://casetext.com/case/stengart-v-loving-care-agency-inc.

[15] Stengart v. Loving Care Agency, Inc.

[16] Pure Power Boot Camp, Inc. v. Warrior Fitness Boot Camp, LLC, 813 F. Supp. 2d 489, 80 Fed. R. Serv. 3d 1025 (S.D.N.Y. 2011). Retrieved January 26, 2023, https://casetext.com/case/pure-power-boot-camp-v-warrior-fitness-boot-camp-2.

and Nancy Baynard. Accusations arose that PPBC accessed and printed emails from Fell's personal and work accounts, which included platforms like Hotmail, Gmail, and WFBC. This case pivoted on whether Brenner violated the Stored Communications Act (SCA) or 18 U.S.C.S. § 2701(a), in the course of these actions. While Brenner's actions were in violation, the court did not find substantive SCA claims present, resulting in a "not guilty" verdict.[17]

Jennings vs. Jennings, a case from 2012, offers another SCA-related ruling, centered around Gail and Lee Jennings, a married.[18] Gail discovered a flower card in Lee's car, indicating another woman's involvement. This prompted a confrontation where Lee admitted to being in love with another woman, communicated frequently through email. Gail disclosed this situation to Holly Broome, her daughter-in-law, who had prior knowledge of Lee's personal Yahoo! email account from her previous work. Broome managed to access Lee's account by correctly guessing security questions, subsequently disseminating the emails to Gail's attorney and private investigator. This breach led to a lawsuit by Lee against Gail, Broome, and others, encompassing charges of invasion of privacy, conspiracy, and violations of the South Carolina Homeland Security Act. The central query in this case revolved around whether the emails were in electronic storage according to the SCA. The circuit court favored the defendants on all counts, including SCA, while the court of appeals upheld the ruling except for Broome. This reversal found Broome in violation of the SCA due to the electronic storage of the emails.[19]

Ultimately, these cases establish pivotal precedents for current and future legal actions and legislations.[20] The assimilation of insights from past rulings empowers both the judicial system and organizations to apply this wisdom to forthcoming scenarios, thus enabling the most judicious decisions possible.

3.2. Current Legislation Landscape

The use of algorithmic management in the workplace, powered by artificial intelligence, presents a multifaceted issue, with its appropriateness hinging on various factors.[21] As employee monitoring technology gains traction in work environments, it becomes imperative to comprehend the existing legal framework and precedents governing its usage, especially considering monitoring exceptions.

---

[17] Pure Power Boot Camp, Inc. v. Warrior Fitness Boot Camp, LLC.

[18] Jennings v. Jennings, 401 S.C. 1, 736 S.E.2d 242 (S.C. 2012). Retrieved January 26, 2023, https://casetext.com/case/jennings-v-jennings-55.

[19] Jennings v. Jennings.

[20] Melissa Medina, "The Stored Communications Act: An Old Statute for Modern Times," *American University Law Review* 63, no. 1 (2013): 267.

[21] Mohammad Hossein Jarrahi et al., "Algorithmic management in a work context," *Big Data & Society* 8, no. 2 (2021): 2.

Algorithmic management holds potential benefits for employers, including heightened efficiency, amplified productivity, and diminished labor costs.[22] By instituting workforce management systems, organizations can streamline operations and optimize resource allocation, culminating in favorable outcomes for both the enterprise and its workforce. However, a host of concerns accompanies algorithmic management, primarily concerning employees.[23] Worries encompass potential bias and discrimination embedded within algorithms, particularly during performance assessment and decision-making. Moreover, the risk of prioritizing efficiency over employee well-being and job satisfaction looms large.[24] A judicious approach entails organizations meticulously evaluating algorithmic management's potential risks and rewards, which underscores the value of being cognizant of current legislation and laws surrounding monitoring practices.

For instance, the Electronic Communications Privacy Act of 1986,[25] a federal statute, empowers employers to monitor employees' verbal and written communications under specific conditions. Certain state laws further regulate such practices. This act enables employers to utilize employee monitoring technology to track real-time employee locations and activities, provided such monitoring remains within reasonable bounds.[26] Moreover, the act permits business owners to monitor all employee verbal and written communications, as long as a legitimate business rationale supports the endeavor. It also allows additional monitoring if

[22] Katherine C. Kellogg, Melissa A. Valentine, and Angele Christin. "*Algorithms at work: The new contested terrain of control*." *Academy of Management Annals* 14, no. 1 (2020): 366.

[23] Daniel Gray, "Algorithmic management in the workplace // AI in the Workplace," Taylor Vinters, August 22, 2022, https://www.taylorvinters.com/article/algorithmic-management-in-the-workplace. See also, Eliane Léontine Bucher, Peter Kalum Schou, and Matthias Waldkirch, "Pacifying the algorithm–Anticipatory compliance in the face of algorithmic management in the gig economy," *Organization* 28, no. 1 (2021): 45.

[24] Gray, "Algorithmic."

[25] The Electronic Communications Privacy Act of 1986 stands as a pivotal federal statute that shapes the boundaries of employer monitoring practices. It grants employers the authority to monitor employees' verbal and written communications under specific conditions, while some states offer additional protections. While this act provides legal groundwork for monitoring, the ethical implications of such practices must be weighed against privacy concerns. Furthermore, recent legislative developments, such as the European Union's GDPR and the California Consumer Privacy Act, emphasize the growing importance of transparency and accountability in the realm of employee monitoring. As the legal landscape continues to evolve, employers must navigate these regulations carefully while maintaining ethical considerations to foster a balanced and respectful work environment.

[26] Jan H. Samoriski, John L. Huffman, and Denise M. Trauth, "Electronic mail, privacy, and the Electronic Communications Privacy Act of 1986: Technology in search of law," *Journal of Broadcasting & Electronic Media* 40, no. 1 (1996): 70.

employees grant consent.[27] Generally, U.S. law has been supportive of employers engaging in robust employee monitoring, provided clear communication to employees underscores these activities, rendering them aware. However, this practice raises the ethical concerns alluded to earlier, even if it is legally permissible.[28]

Furthermore, numerous states boast laws more protective of employee privacy than federal statutes.[29] Employers should be well-versed in recent legislation relating to notifying employees about electronic monitoring. Depending on location, legal obligations may extend to adhering to specific regulations, such as the California Consumer Privacy Act for instance, implemented a law on May 7, 2022, mandating employers to notify employees about electronic monitoring. This law amends the New York Civil Rights Law, impacting all private employers in the state, necessitating conspicuous notice provision to employees upon hire and through a "conspicuous place" like a company intranet.[30] Additionally, California has introduced the California Consumer Privacy Act (CCPA), compelling employers to inform employees about the categories of personal data they collect and the purposes behind such collection.[31] The California Privacy Rights Act of 2020 (CPRA),[32] which took effect on January 1, 2023, further strengthens these regulations, now encompassing employment data. While these laws generally

[27] United States, Congress, House, Committee on the Judiciary, Subcommittee on Courts, Civil Liberties, and the Administration of Justice. *Electronic Communications Privacy Act: Hearings Before the Subcommittee on Courts, Civil Liberties, and the Administration of Justice of the Committee on the Judiciary, House of Representatives, Ninety-ninth Congress, First and Second Sessions, on HR 3378... September 26, October 24, 1985, January 30, and March 5, 1986*. Vol. 4. US Government Printing Office, (1986).

[28] Alder G. Stoney. "Ethical issues in electronic performance monitoring: A consideration of deontological and teleological perspectives." *Journal of Business Ethics* 17 (1998): 729-743.

[29] Daniel J. Solove and Chris Jay Hoofnagle, "A Model Regime of Privacy Protection," *University of Illinois Law Review* 2006, no. 2 (2006): 358. See also, Valerio De Stefano and Simon Taes, "Algorithmic management and collective bargaining," *Transfer: European Review of Labour and Research* 29, no. 1 (2023): 22.

[30] Joshua H. Lerner et al., "New Rules and Risks in Employee Monitoring," *WilmerHale*, June 28, 2022, https://www.wilmerhale.com/insights/client-alerts/20220628-new-rules-and-risks-in-employee-monitoring.

[31] Lothar Determann and Jonathan Tam, "Employers Must Prepare Now For New California Employee Privacy Rights," *Baker McKenzie*, January 3, 2022, https://www.theemployerreport.com/2022/01/employers-must-prepare-now-for-new-california-employee-privacy-rights/.

[32] The California Privacy Rights Act of 2020 (CPRA) is a significant advancement in enhancing privacy rights for California residents. Expanding on the California Consumer Privacy Act (CCPA), CPRA introduces measures like the California Privacy Protection Agency, strengthening regulatory enforcement. It broadens personal data protection, granting individuals control over corrections to their data, and emphasizes safeguarding minors' data. CPRA underscores California's commitment to reinforcing privacy rights in the digital era, setting a precedent for potential legislation elsewhere.

permit technology use for employee performance monitoring, constraints exist, with some cases reaching the Supreme Court.

A series of Supreme Court cases have tackled the legal aspects of employee monitoring, such as City of Ontario v. Quon.[33] This case delved into the extent of privacy rights applicable to electronic communications in a government workplace, centering on a police department's search of an officer's text messages on a city-issued pager. The Court ruled the search reasonable, as the employer had a legitimate interest in monitoring work-related pager usage without excessive intrusion.[34] While these cases and state-enshrined acts underscore the legal contours of employee monitoring, they concurrently underscore other ethical considerations within the workplace. Another case, National Labor Relations Board v. Purple Communications, Inc.[35], revolved around an employer's policy barring non-work-related use of company email. The Supreme Court held that employees possess the right to employ company email for protected activities, including union organizing, under the National Labor Relations Act.[36] These cases typify the intricate legal landscape enveloping employee monitoring and emphasize the necessity for employers to seek legal counsel when instituting monitoring policies.

3.3. Ethical Dilemmas Arising

Data privacy apprehensions expose workers to the sharing of their biometric data with employers, laying bare personal aspects such as religious beliefs, health status, and family particulars.[37] Instances of this have materialized through initiatives like Ford's use of wristbands for maintaining social distancing among factory employees[38] and Amazon's adoption of biometric tracking for drivers to

[33] City of Ontario v. Quon, 560 U.S. 746, 130 S. Ct. 2619, 177 L. Ed. 2d 216 (2010). Retrieved January 26, 2023, https://casetext.com/case/ontario-v-quon.

[34] City of Ontario v. Quon.

[35] "National Labor Relations Board v. Purple Communications, Inc. Retrieved January 26, 2023, https://www.nlrb.gov/case/21-RC-091531.

[36] This act's provisions guarantee employees the right to use company email for concerted activities, including union organizing. The NLRA's application to electronic communication underscores the evolving nature of workplace interactions in the digital age. While the NLRA upholds employees' rights, organizations must navigate a complex landscape to respect these rights while maintaining efficient operations. Striking this balance requires a comprehensive understanding of the NLRA's implications and a commitment to fostering transparent and fair communication channels within the workplace.

[37] Sandra Wachter and Brent Mittelstadt, "A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI," *Columbia Business Law Review* 2019, no. 2 (2019): 494.

[38] Keith Naughton, "Ford Tests Buzzing Wristbands to Keep Workers at Safe Distances," *Bloomberg*, April 16, 2020, https://www.bloomberg.com/news/articles/2020-04-15/ford-tests-buzzing-distancing-wristbands-to-keep-workers-apart?in_source=embedded-checkout-banner.

avert accidents.[39] The application of artificial intelligence in this context can be perceived as intrusive, leading entities like Microsoft and Barclays to anonymize their data.[40] Nonetheless, it can be posited that the ethical quandaries tied to biometric data tracking are indispensable for specific safety measures that necessitate such technological intervention. For instance, Uber employs real-time identification checks to safeguard app users, demonstrating both affirmative and negative facets of employee monitoring technology.[41] The ethical terrain here is nebulous, as employee data might be leveraged to assist or safeguard others at the potential expense of the employee.

Furthermore, the integration of artificial intelligence in workplaces has the potential to inadvertently perpetuate discriminatory biases.[42] This phenomenon is particularly pronounced in new automated hiring processes, where artificial intelligence makes determinations based on historical data. The labor force has historically grappled with racial and gender-based discrimination, a concern that endures via implicit biases and personal preconceptions.[43] By relying on historical data for algorithmic application screening, job candidates who have historically faced discrimination remain sidelined. For instance, algorithms might automatically eliminate graduates of Historically Black Colleges and Universities (HBCUs) due to past patterns of non-hiring from such institutions.[44]

Moreover, artificial intelligence's incorporation into the workforce has ramifications for the gig economy, a sector prominently populated by lower-income workers and marginalized groups.[45] Operating on customer survey inputs

[39] Frank Hersey, "Amazon Selects BehavioSec biometrics for authentication of customer service staff," *Biometric Update*, August 13, 2021, https://www.biometricupdate.com/202108/amazon-selects-behaviosec-biometrics-for-authentication-of-customer-service-staff.

[40] Leonie Cater and Melissa Heikkilä, "Your boss is watching: how AI-powered surveillance rules the workplace, " *Politico*, May 27, 2021, https://www.politico.eu/article/ai-workplace-surveillance-facial-recognition-software-gdpr-privacy/.

[41] M. Keith Chen et al., "The value of flexible work: Evidence from Uber drivers," *Journal of political economy* 127, no. 6 (2019): 2735.

[42] Philipp Hacker, "Teaching fairness to artificial intelligence: Existing and novel strategies against algorithmic discrimination under EU law," *Common Market Law Review* 55, no. 4 (2018): 1143.

[43] Anja Lambrecht and Catherine Tucker, "Algorithmic bias? An empirical study of apparent gender-based discrimination in the display of STEM career ads," *Management science* 65, no. 7 (2019): 2966.

[44] Jessica Shakesprere, Batia Katz, and Pamela J. Loprest, "Racial equity and job quality: causes behind racial disparities and possibilities to address them," *Urban Institute*, September 9, 2021, https://policycommons.net/artifacts/1815047/racial-equity-and-job-quality/2551344/.

[45] Jeremias Adams-Prasll, "What if your boss was an algorithm? economic incentives, legal challenges, and the rise of artificial intelligencie at work," *Comparative labor law and policy journal* 41, no. 1 (2019): 144.

for managerial decisions, this heightened surveillance can engender stress among workers and inhibit collective action.[46] Occupations like Uber driving exemplify how artificial intelligence's management applications intersect with the gig economy. In this scenario, oversight predominantly hinges on customer data and reviews, permitting implicit and explicit biases to influence workers' livelihoods without sufficient accountability. However, legal actions have already emerged in response to this new technology, prompting initiatives aimed at mitigating discrimination through strategic inclusive programming to advance equity and accountability.[47]

Lastly, despite artificial intelligence's intended role in boosting efficiency and refining organizational operations, it has inadvertently fostered distrust and disengagement among employees.[48] The heightened scrutiny of perpetual monitoring has led to diminished employee morale and paradoxically escalated unethical conduct. Furthermore, employees have become more fixated on appearing task-focused for compliance purposes rather than genuinely being productive. This paradox played out at MetLife, a life insurance firm, in 2017, when excessive monitoring led employees to rigidly follow protocol, causing the company to overlook providing benefits to 13,500 customers. In such cases, a reliance on human intelligence and insight superseded automated practices.[49] In lieu of this, organizations should pivot toward cultivating transparency, fairness, accountability, and trust in workplace relationships and interactions.

3.4. Future Impact and Strategies

The trajectory set forth in the preceding sections illuminates a nuanced narrative surrounding the integration of artificial intelligence in employee monitoring, particularly highlighted by the case of MetLife and corroborated by recent research from Harvard University. This narrative is emblematic of the evolving landscape that demands careful consideration to guide future strategies for the symbiotic relationship between technology and workplace ethics. The empirical evidence mirrors the paradoxical impact of surveillance on employee

[46] Shakesprere, Katz, Loprest, "Racial equity,"

[47] Meredith Whittaker et al., *AI now report 2018* (New York: AI Now Institute at New York University, 2018), 26.

[48] Stephen Jackson and Niki Panteli, "Trust or mistrust in algorithmic grading? An embedded agency perspective," *International Journal of Information Management* 69 (2023):12.

[49] A case involving MetLife exemplifies how strict adherence to rules can lead to unintended failures and regulatory penalties. Although data-driven "people analytics" offer potential benefits for better team dynamics and ethical choices, ethical considerations remain crucial. The delicate balance between surveillance and ethics is complex, particularly in the U.S. where the employer's advantage in power dynamics and legal protections allows for extensive employee monitoring through provided devices, emphasizing the need to navigate ethical dimensions in workplace surveillance.

behavior, echoing the findings of a recent study by Thiel et al. from Harvard University.[50] Counterintuitively, intensified monitoring has been shown to inadvertently foster a climate conducive to unethical conduct, implying a diminished sense of personal accountability.

However, these research findings appear to contradict the conclusions drawn by Manokha, who asserted that technological surveillance significantly bolsters employers' disciplinary authority.[51] These technologies empower employers to amplify both the intensive and extensive utilization of workers, leading to substantial upticks in employee productivity. The study additionally implied that the deployment of artificial intelligence serves to augment employers' disciplinary dominion, facilitated by the constant surveillance enabled by modern methods, even in the supervisor's physical absence. Despite this seemingly contradictory revelation, Blum anticipates that in the forthcoming years, employee monitoring might evolve into a more personalized and potentially more invasive dimension, driven by the ongoing trend of remote work arrangements.[52]

Although monitoring tools can be perceived as a means to enhance employee productivity, efficiency, accountability, and safety, they can concurrently give rise to potential legal quandaries—ranging from invasion of privacy and discrimination to allegations of unfair labor practices, workplace injuries, and uncompensated wages and overtime—owing to the intricacies of state laws.[53] The foremost strategy to preempt these prospective legal issues involves establishing Acceptable Use Policies that outline the permissible scope of employee use of company systems and the extent of privacy they can expect. As advised by Yerby, the responsibility of policy formulation and compliance should not solely rest with the IT department, but instead involve a cross-functional team encompassing Human Resources and Legal Counsel.[54] This collaborative approach ensures that monitoring protocols are expertly devised, encompassing aspects such as the methods of monitoring, the subjects under surveillance, the activities subject to

[50] Chase E. Thiel, Nicholas Prince, and Zhanna Sahatjian, "The (electronic) walls between us: How employee monitoring undermines ethical leadership," *Human Resource Management Journal* 32, no. 4 (2022): 744.

[51] Ivan Manokha, "Surveillance, panopticism, and self-discipline in the digital age," *Surveillance and Society* 16, no. 2 (2018): 220.

[52] Sam Blum, "Employee surveillance is exploding with remote work–and could be the new norm," *HR Brew*, January 19, 2022. https://www.hr-brew.com/stories/2022/01/19/employee-surveillance-is-exploding-with-remote-work-and-could-be-the-new-norm.

[53] Anne E. Villanueva and Crystal D. Barnes, "Every Move You Make: When Monitoring Employees Gives Rise to Legal Risks," *Skadden*, September 21, 2022, https://www.skadden.com/insights/publications/2022/09/quarterly-insights/every-move-you-make.

[54] Johnathan Yerby, "Legal and ethical issues of employee monitoring," *Online Journal of Applied Knowledge Management (OJAKM)* 1, no. 2 (2013): 44.

monitoring, and the data accessible for monitoring reports. For companies with existing policies in place, periodic audits—at least annually—should be conducted to guarantee alignment with established procedures.

Another critical consideration revolves around the imperative for employers to implement safeguards that shield both the business and its employees. These protective measures can take various forms, including engaging legal counsel, instituting comprehensive policies, or securing ownership rights.[55] Employers should be proactive in adopting such precautions, as there are instances where a company might incur vicarious liability for failing to uncover threatening or discriminatory emails transmitted through company computer systems. In crafting email and Internet policies, it is pivotal for anti-discrimination principles to seamlessly intertwine with them.[56] Employers should also reiterate their stance against workplace harassment and violence while formulating these policies. Providing new employees with a well-defined email and internet policy as part of their onboarding package further reinforces a culture of responsible and compliant usage.

4. Conclusion

Studying past cases offers us invaluable insights and lessons that can shape our present and future decisions. Historical legal cases establish precedents that guide forthcoming legal judgments. Through the examination of past cases, legal professionals and judges can deepen their comprehension of legal principles and their historical applications. These precedents also hold significance in the realm of business and management, as they provide business leaders with the means to extract lessons from past case studies, enabling them to identify effective strategies and circumvent common pitfalls. This knowledge empowers organizations to make well-informed choices regarding strategy, operations, and risk management. In essence, delving into past cases equips us with the wisdom to make informed decisions, evade typical obstacles, and benefit from the accomplishments and missteps of those who have preceded us.

Legislation against workplace monitoring primarily aims to safeguard employees' privacy and individual liberties within the workplace. This legislative intervention can manifest in various forms, including federal or state laws, regulations, or guidelines. An illustrative instance of such legislation is the Electronic Communications Privacy Act (ECPA), enacted by the US Congress in

[55] Holly Eve, "Three things you must do to safeguard your company," *Forbes*, October 5, 2020. https://www.forbes.com/sites/hollyeve/2020/10/05/three-things-you-must-do-to-safeguard-your-company/?sh=139aa9c968ac.

[56] Yerby, "Legal and ethical issues," 47.

1986. The ECPA delineates parameters for the interception and monitoring of electronic communications, encompassing emails, phone calls, and other digital correspondences. Similarly, legislative measures may encompass constraints on video surveillance, GPS tracking, and alternative methods of workplace monitoring.

The practice of employee monitoring raises a cluster of ethical concerns, notably the violation of privacy. When employees perceive their personal space and privacy rights infringed upon, it prompts feelings of intrusion. Furthermore, employee monitoring can signify a lack of trust between employers and employees, fostering an environment characterized by suspicion that corrodes morale and job satisfaction. Instead, companies should emphasize cultivating transparency, fairness, accountability, and trust in workplace dynamics. Pervasive monitoring often correlates with heightened stress and burnout among employees, fostering an unhealthy work atmosphere. Therefore, employers must carefully weigh the benefits of employee monitoring against potential ethical quandaries, implementing monitoring mechanisms that uphold employee privacy and autonomy.

Looking ahead, employee monitoring might evolve into a more personalized and intrusive realm, potentially inviting legal challenges encompassing privacy violations, discriminatory practices, allegations of unjust labor practices, workplace incidents, and unpaid compensation and overtime. To navigate these impending challenges, companies should establish Acceptable Use Policies elucidating employees' permissibility in utilizing company systems and the extent of privacy they can anticipate. Additionally, employers should institute safeguards to shield both the organization and its workforce, which could encompass retaining legal counsel, formulating comprehensive protocols, or securing ownership rights. Moreover, the formulation of email and Internet policies should seamlessly integrate anti-discrimination principles, and new employees should be furnished with these policies as part of their onboarding package.

References

Adams-Prasll, Jeremias. "What if your boss was an algorithm? economic incentives, legal challenges, and the rise of artificial intelligencie at work." *Comparative labor law and policy journal* 41, no. 1 (2019): 123-146.

Ajunwa, Ifeoma, Kate Crawford, and Jason Schultz. "Limitless worker surveillance." *California Law Review* 105, no. 3 (2017): 735-776.

Aloisi, Antonio, and Valerio De Stefano. "Essential jobs, remote work and digital surveillance: Addressing the Covid-19 pandemic panopticon." *International Labour Review* 161, no. 2 (2022): 289-314.

Bhave, Devasheesh P., Laurel H. Teo, and Reeshad S. Dalal. "Privacy at work: A review and a research agenda for a contested terrain." *Journal of Management* 46, no. 1 (2020): 127-164.

Blum, Sam. "Employee surveillance is exploding with remote work–and could be the new norm." *HR Brew*, January 19, 2022. https://www.hr-brew.com/stories/2022/01/19/employee-surveillance-is-exploding-with-remote-work-and-could-be-the-new-norm.

Blumenfeld, Stephen, Gordon Anderson, and Val Hooper. "Covid-19 and employee surveillance." *New Zealand Journal of Employment Relations* 45, no. 2 (2020): 42-56.

Bucher, Eliane Léontine, Peter Kalum Schou, and Matthias Waldkirch. "Pacifying the algorithm–Anticipatory compliance in the face of algorithmic management in the gig economy." *Organization* 28, no. 1 (2021): 44-67.

Button, Mark, and Peter Stiernstedt. "Comparing private security regulation in the European Union." In *The Rise of Comparative Policing*, edited by Jacques de Maillard and Sebastian Roché, 35-51. London: Routledge, 2021.

Cater, Leonie, and Melissa Heikkilä. "Your boss is watching: how AI-powered surveillance rules the workplace." *Politico*, May 27, 2021. https://www.politico.eu/article/ai-workplace-surveillance-facial-recognition-software-gdpr-privacy/.

Chamorro-Premuzic, Tomas. "Can surveillance AI make the workplace safe?." *MIT Sloan Management Review* 62, no. 1 (2020): 13-15.

Chen, M. Keith, Peter E. Rossi, Judith A. Chevalier, and Emily Oehlsen. "The value of flexible work: Evidence from Uber drivers." *Journal of political economy* 127, no. 6 (2019): 2735-2794.

De Stefano, Valerio, and Simon Taes. "Algorithmic management and collective bargaining." *Transfer: European Review of Labour and Research* 29, no. 1 (2023): 21-36.

Determann, Lothar, and Jonathan Tam. "Employers Must Prepare Now For New California Employee Privacy Rights." *Baker McKenzie*, January 3, 2022. https://www.theemployerreport.com/2022/01/employers-must-prepare-now-for-new-california-employee-privacy-rights/.

Eve, Holly. "Three things you must do to safeguard your company." *Forbes*, October 5, 2020. https://www.forbes.com/sites/hollyeve/2020/10/05/three-things-you-must-do-to-safeguard-your-company/?sh=139aa9c968ac.

Fairweather, N. Ben. "Surveillance in employment: The case of teleworking." In *Computer Ethics*, edited by John Weckert, 381-391. London: Routledge, 2017.

Ferrel, Odies C., and John Fraedrich. *Business ethics: Ethical decision making and cases*. Canada: Cengage learning, 2021.

Gray, Daniel. "Algorithmic management in the workplace // AI in the Workplace." *Taylor Vinters*, August 22, 2022. https://www.taylorvinters.com/article/algorithmic-management-in-the-workplace.

Hacker, Philipp. "Teaching fairness to artificial intelligence: existing and novel strategies against algorithmic discrimination under EU law." *Common market law review* 55, no. 4 (2018): 1143-1185.

Hagen, Christina S., Leila Bighash, Andrea B. Hollingshead, Sonia Jawaid Shaikh, and Kristen S. Alexander. "Why are you watching? Video surveillance in organizations." *Corporate Communications: An International Journal* 23, no. 2 (2018): 274-291.

Hersey, Frank. "Amazon Selects BehavioSec biometrics for authentication of customer service staff." *Biometric Update*, August 13, 2021. https://www.biometricupdate.com/202108/amazon-selects-behaviosec-biometrics-for-authentication-of-customer-service-staff.

Jackson, Stephen, and Niki Panteli. "Trust or mistrust in algorithmic grading? An embedded agency perspective." *International Journal of Information Management* 69 (2023): 102555.

Jarrahi, Mohammad Hossein, Gemma Newlands, Min Kyung Lee, Christine T. Wolf, Eliscia Kinder, and Will Sutherland. "Algorithmic management in a work context." *Big Data & Society* 8, no. 2 (2021): 20539517211020332.

Kaupins, Gundars, and Malcolm Coco. "Perceptions of internet-of-things surveillance by human resource managers." *SAM Advanced Management Journal* 82, no. 2 (2017): 53-64.

Kellogg, Katherine C., Melissa A. Valentine, and Angele Christin. "Algorithms at work: The new contested terrain of control." *Academy of Management Annals* 14, no. 1 (2020): 366-410.

Lambrecht, Anja, and Catherine Tucker. "Algorithmic bias? An empirical study of apparent gender-based discrimination in the display of STEM career ads." *Management science* 65, no. 7 (2019): 2966-2981.

Lerner, Joshua H., Kirk J. Nahra, Jonathan Rosenfeld, Andrew Stauber, and Ali A. Jessani. "New Rules and Risks in Employee Monitoring." *WilmerHale*, June 28, 2022. https://www.wilmerhale.com/insights/client-alerts/20220628-new-rules-and-risks-in-employee-monitoring.

Manokha, Ivan. "Surveillance, Panopticism, and Self-Discipline in the Digital Age." *Surveillance & Society* 16, no. 2 (2018): 219-237.

Medina, Melissa. "The Stored Communications Act: An Old Statute for Modern Times." *American University Law Review* 63, no. 1 (2013): 267-305.

Moussa, Mahmoud. "Monitoring employee behavior through the use of technology and issues of employee privacy in America." *Sage Open* 5, no. 2 (2015): 2158244015580168.

Naim, Mohammad Faraz. "Revamping workplace learning and development during Covid-19 in HR consulting industry in India: a thematic analysis." *International Journal of Knowledge and Learning* 16, no. 3 (2023): 274-289.

Nappi, Ingrid, and Gisele de Campos Ribeiro. "Internet of Things technology applications in the workplace environment: A critical review." *Journal of Corporate Real Estate* 22, no. 1 (2020): 71-90.

Naughton, Keith. "Ford Tests Buzzing Wristbands to Keep Workers at Safe Distances." *Bloomberg*, April 16, 2020. https://www.bloomberg.com/news/articles/2020-04-15/ford-tests-buzzing-distancing-wristbands-to-keep-workers-apart?in_source=embedded-checkout-banner.

Nemeth, Charles P. *Private security and the law*. Boca Raton: CRC Press, 2017.

Saatçi, Banu, Roman Rädle, Sean Rintel, Kenton O'Hara, and Clemens Nylandsted Klokmose. "Hybrid meetings in the modern workplace: stories of success and failure." In *Collaboration Technologies and Social Computing: 25th International Conference, CRIWG+ CollabTech 2019, Kyoto, Japan, September 4–6, 2019, Proceedings 25*, pp. 45-61. Springer International Publishing, 2019.

Samoriski, Jan H., John L. Huffman, and Denise M. Trauth. "Electronic mail, privacy, and the Electronic Communications Privacy Act of 1986: Technology in search of law." *Journal of Broadcasting & Electronic Media* 40, no. 1 (1996): 60-76.

Shakesprere, Jessica, Batia Katz, and Pamela J. Loprest. "Racial equity and job quality: causes behind racial disparities and possibilities to address them." *Urban Institute*, September 9, 2021. https://policycommons.net/artifacts/1815047/racial-equity-and-job-quality/2551344/.

Solove, Daniel J., and Chris Jay Hoofnagle. "A Model Regime of Privacy Protection." *University of Illinois Law Review* 2006, no. 2 (2006): 357-404.

Thiel, Chase E., Nicholas Prince, and Zhanna Sahatjian. "The (electronic) walls between us: How employee monitoring undermines ethical leadership." *Human Resource Management Journal* 32, no. 4 (2022): 743-758.

Villanueva, Anne E., and Crystal D. Barnes. "Every Move You Make: When Monitoring Employees Gives Rise to Legal Risks." *Skadden*, September 21, 2022. https://www.skadden.com/insights/publications/2022/09/quarterly-insights/every-move-you-make.

Wachter, Sandra, and Brent Mittelstadt. "A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI." *Columbia Business Law Review* 2019, no. 2 (2019): 494-620.

Whittaker, Meredith, Kate Crawford, Roel Dobbe, Genevieve Fried, Elizabeth Kaziunas, Varoon Mathur, Sarah Mysers West, Rashida Richardson, Jason Schultz, and Oscar Schwartz. *AI now report 2018*. New York: AI Now Institute at New York University, 2018.

Yerby, Johnathan. "Legal and ethical issues of employee monitoring." *Online Journal of Applied Knowledge Management (OJAKM)* 1, no. 2 (2013): 44-55.

Zickuhr, Kathryn. "Workplace surveillance is becoming the new normal for US workers." *Washington Center for Equitable Growth*, August 17, 2021. https://equitablegrowth.org/research-paper/workplace-surveillance-is-becoming-the-new-normal-for-u-s-workers/.