Consent, Privacy and the Digital Employee: Ethical Boundaries of AI Data Collection in Workplace Learning Platforms

Wuraola Balqees Ogidan
Department of Sociology, University of Lagos, Nigeria

Patience Nyong Asikpo
Department of Sociology, Landmark University, Omu-Aran, Kwara State, Nigeria

Josephine Aiyemekhiu Ogbatue
Department of Communication Management, Delta State University, Abraka, Nigeria

Abstract
Artificial intelligence is increasingly embedd--ed in workplace learning platforms through adaptive training systems, skills intelligence tools,learning analytics dashboards, automated assessment,intelligent tutoring,recommendati--on engines, and predictive workforce develo--ment systems. These technologies promise personalised learning, improved capability development, efficient compliance training, and evidence-based human resource planning. However, they also intensify the collection, processing, profiling, and secondary use of employee data. In AI-enabled learning environments, the employee is no longer merely a learner but a continuously observed and datafied subject whose behaviours, preferences,performancepatterns,competencies errors, interactions, and development trajectories may be converted into managerial intelligence. This paper examines the ethical boundaries of AI data collection in workplace learning platforms, focusing on consent, privacy,power imbalance, employee autonomy, transparency,purposelimitation,dataminimisation, algorithmic bias, and organisational accountability. The paper adopts a conceptual and normative research design, synthesising literature from AI ethics, workplace learning, employment relations, data protection, surveillance studies, and algorithmic manage--ment. It argues that conventional consent models are ethically insufficient in workplace learning because employment relations are characterised by dependency, hierarchy, and unequal bargaining power. Employees may formally consent to data collection while lacking genuine freedom to refuse, withdraw, or contest AI-enabled monitoring. The paper proposes an Ethical Boundary Framework for AI-Enabled Workplace Learning Platforms based on six principles: contextual consent, privacy by design, proportionality, purpose limitation, employee agency, and accountable governance.
The framework distinguishes between learning-supportive analytics and surveillance-oriented analytics and recommends clear organisational separation between developme--ntal learning data and punitive employment decision-making. The paper contributes to the literature by reframing workplace learning platforms as socio-technical governance systems rather than neutral educational tools. It concludes that ethical AI adoption in workplace learning requires a shift from data extraction to data stewardship, where employee dignity, trust, autonomy, and fairness are treated as core conditions of sustainable organisational learning.

Keywords:
artificial intelligence; workplace learning; employee privacy; digital employee; consent; learning analytics; workplace surveillance; algorithmic management; AI governance; data ethics.

1. Introduction

Digital transformation has altered the structure, delivery, and governance of

DOI: https://doi.org/10.5281/zenodo.20639001

workplace learning. Organisations increasingly use learning management systems, learning experienceplatforms,microlearningapplications adaptive training tools, skills intelligence systems, virtual coaching assistants, and AI-supported assessment systems to train and manage employees.

These tools are often promoted as mechanisms for improving productivity, personalising professional development, supporting compliance,and aligning employee capabilities with organisational strategy (Ifenthaler & Yau, 2020; Williamson, 2017). In contemporary organisations, learning is no longer limited to classroom training, workshops, mentoring, or self-directed study. It is increasingly mediated by data-driven platforms that continuously record, analyse, classify, and predict employee learning behaviour. The rise of artificial intelligence in workplace learning has intensified this transformation. AI-enabled learning platforms can recommend courses, detect skills gaps, predict learning outcomes, identify employees suitable for particular roles, automate feedback, generate personalised learning pathways, and support organisational talent analytics (OECD, 2023; Tursunbayeva et al., 2021). These functions depend on extensive data collection. Platforms may gather information about course completion, assessment results, time spent on modules, login frequency, discussion-board participation, peer feedback, search histories, document engagement, quiz attempts, response patterns, error rates, badges, certifications, and behavioural indicators of engagement. More advanced systems may process communication data, sentiment, psychometric information, biometric signals, or affective cues (Crawford, 2021; Moore, 2020). As a result, workplace learning platforms are becoming powerful data infrastructures within organisational life.

This development gives rise to the figure of the "digital employee." The digital employee is not simply an employee who uses digital tools. Rather, the digital employee is an organisational subject whose identity, value, potential, and risk are partly constructed through data traces. In AI-enabled learning platforms, the employee becomes visible to the organisation as a data profile: a set of scores, classifications, behavioural signals, predicted competencies, skills gaps, compliance risks, and developmental recommendations. These data profiles may support learning, but they may also influence managerial judgement, performance evaluation, promotion decisions, succession planning, workforce restructuring, and disciplinary processes (Ajunwa, 2020; Kellogg et al., 2020). The central ethical issue is therefore not whether AI can improve workplace learning. In many cases, AI may provide real benefits. It can make learning more personalised, identify training needs more quickly, improve accessibility, support just-in-time development, and help organisations respond to rapidly changing skills requirements (OECD, 2019, 2023). The ethical issue is whether the data practices that make AI-enabled learning possible respect employee autonomy, privacy, dignity, fairness, and trust. A workplace learning platform may be presented as a developmental tool while simultaneously functioning as an infrastructure of surveillance and control (Ball, 2021; Lyon, 2018; Zuboff, 2019).

Consent is at the centre of this debate. In many digital systems, consent is treated as a legitimising mechanism. Users are informed of data practices and asked to accept terms and conditions. However, the employment context complicates this model. Employees are not ordinary consumers. They operate within hierarchical relationships and may depend on employers for income, promotion, benefits, professional identity, and long-term career opportunities. The European Data Protection Board (2020) explains that employee consent may not be freely given where there is a clear imbalance of power between employer and employee. This means that a formal act of agreement may not amount to genuine ethical consent. Privacy is equally contested. Workplace learning data may initially appear harmless because it concerns training rather than intimate personal life. However, learning data can reveal sensitive information about cognitive performance, behavioural discipline, motivation,professional ambition, adaptability, confidence, communication patterns, language proficiency, disability-related needs, emotional responses, and perceived competence (Prinsloo & Slade, 2017; Slade & Prinsloo, 2013). When combined with human resource data, productivity metrics, communication records, or psychometric assessments, learning data can become a basis for intrusive profiling (Khan & Tang, 2016; Tursunbayeva et al., 2021). The ethical risk increases when employees do not know what is collected, how

DOI: https://doi.org/10.5281/zenodo.20639001

long it is stored, who has access, how algorithms interpret it, or whether it will affect employment outcomes. Recent regulatory and policy developments reinforce the importance of this problem. The European Union's Artificial Intelligence Act establishes a risk-based framework for AI governance and identifies employment-related AI systems as high-risk where they may significantly affect people's livelihoods and rights (European Parliament and Council of the European Union, 2024). The General Data Protection Regulation also emphasises principles such as lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity, confidentiality, and accountability (European Parliament and Council of the European Union, 2016). These principles are highly relevant to AI-enabled workplace learning because such systems process employee data in contexts where organisational power and individual vulnerability intersect.

This paper examines the ethical boundaries of AI data collection in workplace learning platforms. It asks: What ethical principles should govern AI-driven data collection in workplace learning platforms to protect employee consent, privacy, and agency? The paper develops a conceptual framework for responsible AI data governance in workplace learning environments. It argues that organisations must move beyond compliance-oriented consent forms and adopt a stewardship model that treats employee data as relational, contextual, and ethically sensitive.

2. Literature Review

2.1 Workplace learning in the age of AI

Workplace learning has traditionally been understood as the process through which employees acquire, update, and apply knowledge, skills, and professional capabilities within organisational contexts. It includes formal training, informal learning, mentoring, peer interaction, reflective practice, job rotation, coaching, and experiential learning. The digitalisation of workplace learning has expanded the scale and visibility of learning activity. Learning management systems allow organisations to assign courses, track completion, document compliance, and standardise training delivery. Learning experience platforms add personalisation, social learning, recommendation systems, and content aggregation. AI-enabled systems go further by using machine learning, natural language processing, predictive analytics, and automated decision support (Ifenthaler & Yau, 2020; Selwyn, 2019). AI in workplace learning can provide several benefits. It can recommend learning materials based on role, skill level, career goals, or organisational needs. It can identify gaps between current and desired competencies. It can support adaptive learning by adjusting content difficulty based on performance. It can provide automated feedback and tutoring. It can help organisations map workforce capabilities and plan reskilling programmes (OECD, 2023). In sectors experiencing rapid technological change, such systems may support continuous learning and organisational resilience.

However, AI-enabled learning also changes the nature of workplace learning. Learning becomes increasingly data-driven, measurable, and comparable. Activities that were previously informal or invisible can become recorded and evaluated. Employees may become aware that their learning behaviour is being tracked and may adjust their behaviour accordingly. The platform does not merely deliver learning; it structures the conditions under which learning is observed, interpreted, and governed (Williamson, 2017). This transformation has important ethical implications. Workplace learning is supposed to support development, experimentation, and growth. Learning often involves mistakes, uncertainty, hesitation, and vulnerability. If every learning action is recorded and potentially used in employment decisions, employees may become less willing to experiment or expose gaps in knowledge. The developmental function of learning may be undermined by the evaluative function of data analytics (Prinsloo & Slade, 2017; Slade & Prinsloo, 2013).

2.2 Learning analytics and datafication

Learning analytics is commonly defined as the measurement,collection,analysis, and reporting of data about learners and their contexts for purposes of understanding and optimising learning. In educational settings, learning analytics has generated debate about student privacy, informed consent, data ownership, predictive profiling, bias, intervention, and institutional responsibility (Ifenthaler & Yau, 2020; Prinsloo & Slade, 2017; Slade &

DOI: https://doi.org/10.5281/zenodo.20639001

Prinsloo, 2013). These concerns become even more complex in workplace contexts because learning data may be linked to employment consequences. Datafication refers to the process through which human activities are translated into quantifiable data. In workplace learning platforms, datafication occurs when learning behaviour is converted into measurable indicators such as engagement scores, completion rates, competency ratings, time-on-task,participationfrequency,
knowledge checks, assessment scores, confidence levels, and predictive readiness indicators (Dencik et al., 2019; Williamson, 2017). These indicators may appear objective, but they are constructed through design choices. What the platform measures becomes what the organisation sees. What is not measured may be ignored.

A key problem is that learning analytics may produce simplified representations of complex learning processes. For example, an employee who spends less time on a module may already know the content, may be highly efficient, or may be disengaged. An employee who fails an assessment may lack knowledge, may have experienced technical problems, may be working in a second language, or may have misunderstood the question format. An employee who rarely participates in discussion forums may be shy, overworked, culturally cautious, or assigned to a role with limited time for online interaction. Without contextual interpretation, analytics can generate misleading conclusions (Köchling & Wehner, 2020; Martin, 2019). Learning analytics also creates risks of behavioural control. Employees may learn to perform for the platform rather than for genuine development. They may click through modules, optimise completion metrics, avoid difficult courses, or prioritise visible learning activity over meaningful skill acquisition. In workplace learning, the ethical problem is that data collection can alter the behaviour it claims to observe. This concern reflects broader critiques of surveillance capitalism and data-driven behavioural control (Lyon, 2018; Zuboff, 2019).

2.3.Consent and the employment relationship

Consent is often treated as a central basis for legitimate data processing. Ethically, consent requires more than a signed form or digital checkbox. It requires that individuals understand what they are agreeing to, have meaningful choice, are free from coercion, can refuse without penalty, and can withdraw without negative consequences (European Data Protection Board, 2020). These requirements are difficult to satisfy in the employment relationship. Employees may feel obliged to accept data collection because the employer controls access to work, income, benefits, professional opportunities, and evaluation. Even when a learning platform is officially optional, employees may believe that non-participation will be interpreted as lack of commitment. If managers encourage employees to use the platform, refusal may carry reputational or career costs. If completion data is linked to performance reviews, the platform becomes functionally mandatory (Ball, 2021; Moore, 2020).

The power imbalance between employer and employee means that workplace consent must be treated cautiously. The European Data Protection Board (2020) states that consent in employment is problematic because workers may not be able to refuse or withdraw consent without fear of adverse consequences. Similarly, workplace privacy literature emphasises that employee agreement may be shaped by dependency and organisational hierarchy (Ajunwa, 2020; Leicht-Deobald et al., 2019). These principles are highly relevant to AI-enabled learning platforms because employees may not be able to opt out of data collection without losing access to required training or career development. Consent is further complicated by AI opacity. Employees may not understand what data the AI system collects, how models process it, what inferences are generated, whether profiles are shared, how long data is stored, or whether data is used to train future models. A privacy notice may disclose categories of processing, but such disclosure may be too abstract to support meaningful understanding (Binns, 2022; Martin, 2019). Employees may consent to “learning analytics” without realising that their behaviour may be used to predict performance risk or promotion readiness.

Therefore, the ethical question is not simply whether employees consented. It is whether the organisation created conditions under which consent could be meaningful. In workplace learning, this requires transparency, granularity, alternatives, non-retaliation,

DOI: https://doi.org/10.5281/zenodo.20639001

withdrawal rights, and limits on secondary use (European Data Protection Board, 2020; Floridi & Cowls, 2022).

2.4 Privacy and workplace surveillance

Privacy in the workplace has always involved tension between organisational interests and employee autonomy. Employers have legitim--ate reasons to collect certain data, such as attendance, compliance, training completion, safetycertification,securitylogs,andperformanc e-related information. However, digital technologies expand the scope, granularity, and persistence of monitoring (Ball, 2021; Lyon, 2018). AI adds predictive and inferential capabilities, allowing organisations not only to record what employees do but also to infer what they may know, feel, intend, or become (Crawford, 2021; Moore, 2020). Workplace surveillance may be overt or hidden, narrow or broad, episodic or continuous, supportive or punitive. AI-enabled learning platforms may contribute to surveillance when they collect detailed behavioural data and make it available to managers. A platform designed for learning can become a surveillance tool if it tracks employees continuously, compares them with peers, flags "low engagement," predicts "low potential," or identifies "non-compliant" behaviour without adequate context (Kellogg et al., 2020; Sánchez-Monedero & Dencik, 2022).

Privacy should not be reduced to secrecy. In workplace learning, privacy also concerns control over self-presentation, freedom to make mistakes, protection from unfair inference, and preservation of boundaries between development and discipline (Prinsloo & Slade, 2017; Slade & Prinsloo, 2013). Employees may accept that employers need evidence of training completion. They may not accept that every hesitation, error, click, or learning preference should become part of a permanent evaluative profile. Surveillance can also produce behavioural conformity. Employees who know they are being monitored may avoid risk, conceal uncertainty, or perform only those behaviours that platforms reward (Lyon, 2018; Zuboff, 2019). In learning environments, this is damaging because authentic learning requires experimentation and the possibility of failure. If employees fear that errors will become permanent data records, the learning platform may weaken rather than strengthen organisational learning.

2.5 Algorithmic management and worker control

Algorithmic management refers to the use of algorithms to allocate tasks, evaluate perfor--mance, discipline workers, predict outcomes, and shape managerial decision-making. It is often associated with platform work, logistics, call centres, warehousing, and gig economy systems, but algorithmic management is increasingly relevant to professional and knowledge work (Kellogg et al., 2020; Newlands, 2021). AI-enabled learning platforms can become part of algorithmic management when they generate data used in human resource decisions. For example, a platform may identify employees who need reskilling,recommendemployees for leadership development, rank workers according to skill-readiness, or flag individuals as compliance risks. These functions can influence opportunity distribution. Employees classified as high potential may receive more training and promotion opportunities; employees classified as low engagement may receive less trust or more scrutiny. The result can be a feedback loop in which data-driven classifications shape future outcomes (Ajunwa, 2020; O'Neil, 2016). Algorithmic management raises concerns about transparency, due process, contestability, and fairness. Employees may not know how decisions are made or how to challenge incorrect data. Managers may over-rely on algorithmic outputs, treating scores and dashboards as objective truth. This can lead to automation bias, where human decision-makers defer to systems even when outputs are incomplete or misleading (Binns, 2022; Martin, 2019).

In workplace learning, algorithmic managem--ent is especially problematic because learning data is developmental by nature. A low score should indicate a need for support, not necessarily a lack of value. If learning analytics are used punitively, employees may become less willing to engage honestly with learning opportunities. Ethical governance must therefore protect the developmental purpose of workplace learning (Prinsloo & Slade, 2017; Tursunbayeva et al., 2021).

2.6 AI governance and regulatory context

DOI: https://doi.org/10.5281/zenodo.20639001

AI governance involves the policies, processes, standards, and accountability mechanisms used to ensure that AI systems are safe, fair, transparent, lawful, and aligned with human values (Floridi & Cowls, 2022; OECD, 2019). In workplace learning, AI governance must address both technical risks and employment-related risks. It must consider data quality, model bias, explainability, cybersecurity, privacy, vendor accountability, employee rights, and organisational culture. The EU AI Act provides an important regulatory reference point because it adopts a risk-based approach to AI and imposes obligations on high-risk systems. AI systems used in employment, worker management, and access to self-employment are treated as high-risk because they can significantly affect people's livelihoods and rights (European Parliament and Council of the European Union, 2024). Although not every learning platform will fall directly under the same regulatory category in every jurisdiction, the ethical logic is clear: AI systems that affect employees' opportunities require heightened scrutiny. The GDPR also provides relevant principles for data processing, including transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity, confidentiality, and accountability (European Parliament and Council of the European Union, 2016). These principles are particularly important in workplace learning because learning data can be repurposed, combined with HR data, or used to produce consequential profiles.

OECD research highlights the need to examine the real organisational and worker-level effects of AI adoption rather than relying only on abstract projections (OECD, 2023). This is important because AI ethics cannot be evaluated only by system design or stated intention. It must also consider lived experience: whether workers understand the system, whether they trust it, whether it changes power relations, whether it creates stress, and whether it supports or undermines meaningful work.

3. Methodology

This paper adopts a conceptual and normative research methodology. It does not collect primary empirical data. Instead, it synthesises existing scholarship and policy literature to develop a framework for evaluating ethical boundaries in AI-enabled workplace learning platforms. A conceptual approach is appropri--ate because the topic sits at the intersection of emerging technology, organisational practice, employment relations, privacy law, and ethics. The ethical issues are not reducible to technical performance or legal compliance; they require normative analysis of power, autonomy, dignity, and fairness (Floridi & Cowls, 2022; Martin, 2019). The paper draws on five bodies of literature. First, it uses workplace learning scholarship to understand the developmental purpose of organisational learning. Second, it uses learning analytics literature to examine how learner data is collected, interpreted, and used (Ifenthaler & Yau, 2020; Slade & Prinsloo, 2013). Third, it uses privacy and data protection scholarship to analyse consent, purpose limitation, minimisation, and accountability (European Data Protection Board, 2020; European Parliament and Council of the European Union, 2016). Fourth, it uses surveillance studies to examine how digital monitoring shapes behaviour and power relations (Ball, 2021; Lyon, 2018; Zuboff, 2019). Fifth, it uses AI ethics and algorithmic management literature to evaluate risks of bias, opacity, automation bias, and worker control (Ajunwa, 2020; Kellogg et al., 2020; Köchling & Wehner, 2020).

The analysis is guided by four normative questions. First, can employees meaningfully understand, refuse, modify, or withdraw from AI data collection? Second, is the data collected necessary, proportionate, secure, and limited to legitimate learning purposes? Third, does the system support employee developm--ent,ordoes it intensify managerial surveillance and control? Fourth, are there mechanisms for explanation, contestation, correction, independent review, and remedy? The paper develops the Ethical Boundary Framework through conceptual synthesis. This means that it identifies recurring ethical principles across the literature and translates them into workplace learning governance requirements.

The framework is intended for researchers, organisational leaders, HR professionals, learning and development specialists, data protection officers, AI governance teams, and platform developers.

4. Ethical Risks of AI Data Collection in Workplace Learning Platforms

DOI: https://doi.org/10.5281/zenodo.20639001

4.1 The illusion of voluntary consent

The first ethical risk is the illusion of voluntary consent. Many workplace learning platforms rely on employees accepting privacy notices or terms of use before accessing training. However, employees may not experience this as a genuine choice. If a platform is required for onboarding, compliance, certification, performance improvement, promotion, or professional development, refusal is not practically available. Even when consent is formally requested, the underlying employment relationship may make consent coercive (European Data Protection Board, 2020; Moore, 2020).

This creates a distinction between formal consent and substantive consent. Formal consent occurs when an employee clicks "accept," signs a form, or acknowledges a policy. Substantive consent occurs when the employee genuinely understands the data practice, has a realistic alternative, can refuse without penalty, and can withdraw without retaliation. In workplace learning platforms, formal consent is common; substantive consent is harder to achieve. The ethical risk is that consent becomes a legitimising fiction. Organisations may claim that employees agreed to data collection while ignoring whether employees had meaningful control. This is especially problematic when data collection extends beyond what is necessary for learning delivery. For instance, employees may reasonably expect the platform to record course completion, but not to analyse emotional engagement, generate productivity predictions, or share behavioural profiles with managers (Ball, 2021; Sánchez-Monedero & Dencik, 2022). A more ethical approach requires layered and contextual consent. Employees should be informed separately about different data uses: platform access, compliance tracking, personalised recommendations, skills analytics, managerial reporting, model training, vendor processing, and research use. Essential processing should be distinguished from optional processing. Employees should not lose access to mandatory training because they refuse non-essential analytics (European Data Protection Board, 2020; Floridi & Cowls, 2022).

4.2 Opaque data collection

The second risk is opacity. AI-enabled platforms may collect more data than employees realise. Some data is visible, such as assessment scores or certificates. Other data is less visible, such as clickstream patterns, time spent on pages, navigation paths, pause frequency, scrolling behaviour, device information, metadata, peer interaction, and inferred engagement. Employees may not know that these signals are collected or how they are interpreted (Crawford, 2021; Williamson, 2017). Opacity undermines autonomy because employees cannot make informed choices about behaviour if they do not understand the monitoring environment. It also undermines trust because employees may later discover that data was collected in unexpected ways. In workplace contexts, hidden or poorly explained monitoring can create suspicion and resistance (Ball, 2021; Lyon, 2018). AI systems also create inferential opacity. Even if employees know that data is collected, they may not understand the inferences generated from that data. A system may infer motivation, readiness, risk, confidence, or potential from behavioural signals. These inferences may be inaccurate, yet still influence decisions. Employees should therefore be informed not only about raw data collection but also about profiling and predictio
n (Binns, 2022; Martin, 2019).

4.3 Function creep and secondary use

Function creep occurs when data collected for one purpose is later used for another. In workplace learning platforms, this is one of the most serious ethical risks. Data collected to support learning may later be used for performancemanagement,promotion decisions, redundancyplanning,disciplinaryinvestigations productivity scoring, or workforce segmentation (Khan & Tang, 2016; Tursunbayeva et al., 2021). For example, a platform may initially collect completion data to ensure compliance training. Over time, managers may use the same data to identify "uncommitted" employees. A skills analytics tool may be introduced to support reskilling but later used to decide who is replaceable. A recommendation engine may collect learning preferences but later contribute to psychological profiling. Each new use may seem minor, but cumulatively the platform becomes a surveillance infrastructure (Lyon, 2018; Zuboff, 2019).

Function creep violates employee expectations and weakens trust. It also conflicts with the

DOI: https://doi.org/10.5281/zenodo.20639001

principle of purpose limitation. Ethical governance requires that organisations define purposes clearly before data collection begins and prevent unauthorised expansion. If new purposes emerge, employees should be informed, impact assessments should be conducted, and renewed consent or another appropriate lawful basis should be established (European Parliament and Council of the European Union, 2016; Floridi & Cowls, 2022).

4.4 Data minimisation failure

AI systems often encourage data maximisation because more data is assumed to improve prediction and personalisation. However, ethical data governance requires minimisation: organisations should collect only what is necessary for a legitimate purpose (European Parliament and Council of the European Union, 2016). Workplace learning platforms may violate this principle when they collect excessive behavioural data, retain data indefinitely, or gather intrusive information without clear necessity. Not all data that is technically useful is ethically justified. For instance, detailed time-on-page data may help optimise content design but may be unnecessary for individual employee evaluation. Facial expression analysis may claim to measure engagement but may be scientifically contested, intrusive, and disproportionate. Keystroke dynamics, attention tracking, and biometric indicators may create harms that outweigh learning benefits (Crawford, 2021; Moore, 2020).

Data minimisation should apply to collection, access, retention, and sharing. It is not enough to collect less data; organisations must also limit who can see it, how long it is stored, whether it is identifiable, and whether it is shared with vendors or managers. These safeguards are essential because data collected for learning may later be combined with other workplace data to produce more intrusive profiles (Ajunwa, 2020; Tursunbayeva et al., 2021).

4.5 Bias and unequal impact

AI-enabled learning platforms may produce biased outcomes if data, models, or interpretations reflect unequal workplace conditions. Employees differ in role, schedule, workload, language background, disability, access to technology, caregiving responsibilities, and digital literacy. These differences can affect learning-platform behaviour without reflecting motivation or ability (Köchling & Wehner, 2020; Leicht-Deobald et al., 2019). For example, employees in frontline roles may have less time for online learning than office-based employees. Older workers may interact differently with digital systems. Employees with disabilities may take longer to complete modules. Employees working night shifts may access training irregularly. Employees using shared devices may generate different usage patterns. If AI systems interpret these differences as lack of engagement or lower potential, they may reproduce workplace inequalities (O'Neil, 2016; West et al., 2019).

Bias can also arise from historical data. If past promotion patterns were biased, AI systems trained on such data may learn to associate certain behaviours, backgrounds, or communication styles with success. In learning platforms, this may influence who receives advanced training recommendations or leadership development opportunities (Ajunwa, 2020; Köchling & Wehner, 2020). Ethical AI requires bias audits, contextual interpretation, and human oversight. It also requires attention to structural conditions. It is unfair to penalise employees for low learning engagement if the organisation does not provide protected learning time, accessible content, or adequate technical support (Floridi & Cowls, 2022; OECD, 2019).

4.6 Psychological safety and learning inhibition

Learning requires psychological safety. Employees must feel able to ask questions, make mistakes, reveal knowledge gaps, and attempt difficult tasks without fear of punishment. AI data collection can undermine psychological safety if employees believe their learning struggles will be permanently recorded and used against them (Prinsloo & Slade, 2017; Slade & Prinsloo, 2013). This risk is especially important in reskilling contexts. Employees asked to learn new technologies may initially perform poorly. If early errors become part of an evaluative record, employees may avoid challenging courses or conceal weaknesses. They may choose easy modules to maintain favourable metrics rather than engage in meaningful development. This produces a paradox: data-

DOI: https://doi.org/10.5281/zenodo.20639001

driven learning systems designed to improve skills may discourage genuine learning (Ifenthaler & Yau, 2020; Selwyn, 2019).
Organisations should therefore protect "safe learning zones." Employees need spaces where learning data is used only for personal feedback and support, not for discipline or ranking. Some data may be aggregated for programme improvement, but individual-level developmental data should be treated with caution. This distinction is necessary to preserve trust in workplace learning systems (Ball, 2021; Moore, 2020).

4.7 Vendor power and third-party data use

Many workplace learning platforms are provided by external vendors. This creates additional risks. Vendors may process employee data for platform functionality, analytics, benchmarking, model training, product improvement, or commercial development. Employees may have little visibility into these arrangements. Employers may also lack full understanding of vendor data practices (Crawford, 2021; Tursunbayeva et al., 2021). Vendor governance is therefore essential. Organisations should examine contracts, data processing agreements, retention policies, security practices, sub-processors, cross-border transfers, model training practices, and deletion procedures. Vendors should not be allowed to use employee data for unrelated purposes without clear authorisation and safeguards (European Parliament and Council of the European Union, 2016; OECD, 2019). AI vendors may also shape organisational norms by designing dashboards, default metrics, and reporting tools. If a platform's default design encourages ranking, comparison, or surveillance, organisations may adopt these practices without deliberate ethical reflection. Procurement decisions should therefore include ethical assessment, not only cost and functionality (Kellogg et al., 2020; Martin, 2019).

4.8 Biometric and affective data risks

Some AI learning systems attempt to measure attention, emotion, stress, engagement, or fatigue using facial analysis, eye tracking, voice analysis, keystroke patterns, or other biometric and behavioural signals. These practices are especially intrusive. They may claim to improve learning, but they also enter deeply personal territory (Crawford, 2021; Moore, 2020). Affective computing in workplace learning raises serious concerns. Emotional expressions are context-dependent and culturally variable. Inferring attention or engagement from facial behaviour may be unreliable. Employees may feel that their bodies and emotions are being monitored by the employer. Such monitoring can damage dignity and trust (Ball, 2021; Lyon, 2018). In most workplace learning contexts, biometric and affective data collection should be considered disproportionate. If an organisation claims such data is necessary, it should face a high burden of justification, independent review, explicit safeguards, and genuine alternatives. In many cases, the ethical boundary should be prohibition rather than regulation.

5. Ethical Boundary Framework for AI-Enabled Workplace Learning Platforms

This paper proposes an Ethical Boundary Framework based on six principles: contextual consent, privacy by design, proportionality, purpose limitation, employee agency, and accountable governance.

Figure 1. Ethical Boundary Framework for AI-Enabled Workplace Learning Platforms

The proposed Ethical Boundary Framework is presented in Figure 1. The figure summarises the six core principles that should guide AI data collection in workplace learning platforms and shows how these principles support responsible data stewardship, employee dignity, trust, autonomy, and fairness.

5.1 Contextual consent

Consent in workplace learning must be contextual rather than generic. Employees should not be asked to provide broad, one-time

DOI: https://doi.org/10.5281/zenodo.20639001

agreement to all current and future data practices. Instead, consent should be specific to particular purposes and sensitive to the employment context (European Data Protection Board, 2020). Contextual consent requires clear distinction between mandatory and optional processing. For example, collecting completion records for legally required safety training may be necessary. Collecting behavioural analytics for personalised recommendations may be optional. Using data for AI model training, benchmarking, or managerial ranking should require separate justification and communication (European Parliament and Council of the European Union, 2016).

Consent should also be layered. Employees should receive concise explanations at the point of use and detailed information in accessible policies. They should be told what data is collected, why it is collected, how it is analysed, who can access it, whether it affects employment decisions, how long it is retained, and how they can exercise rights. Because consent may be weak in employment settings, organisations should not rely on consent alone. They should combine consent with structural safeguards such as minimisation, purpose limitation, independent oversight, and employee consultation (Floridi & Cowls, 2022; Martin, 2019).

5.2 Privacy by design

Privacy by design requires privacy protections to be embedded into platform architecture and organisational processes. It includes technical, organisational, and contractual safeguards (European Parliament and Council of the European Union, 2016). Technical safeguards include data minimisation, pseudonymisation, encryption, access controls, retention limits, secure authentication, audit logs, and privacy-preservinganalytics. Organisational safeguards include clear policies, training for managers, governance committees, and accountability procedures. Contractual safeguards include vendor restrictions, sub-processor controls, deletion requirements, and limits on model training (OECD, 2019; Tursunbayeva et al., 2021). Privacy by design also requires careful dashboard design. Dashboards should avoid unnecessary individual-level surveillance. Managers may need aggregated insights into team training progress, but they do not always need detailed behavioural traces. Employees should have access to their own data and explanations of how it is used (Binns, 2022; Martin, 2019).

5.3 Proportionality

Proportionality requires that data collection be appropriate and limited in relation to the learning objective. Organisations should ask whether the same goal can be achieved through less intrusive means. This principle is consistent with data protection obligations and broader AI ethics frameworks that emphasise necessity, fairness, and respect for human autonomy (European Parliament and Council of the European Union, 2016; Floridi & Cowls, 2022). A proportionality assessment should include five questions. First, what specific learning purpose does the data serve? Second, is the data necessary for that purpose? Third, is there a less intrusive alternative? Fourth, what harms could result from collection, inference, access, or misuse? Fifth, do the benefits justify the risks?

For example, recording course completion for compliance training is likely proportionate. Recording facial expressions to infer attention during routine training is likely disproportionate. Collecting assessment scores for learner feedback may be appropriate; sharing every failed attempt with line managers may not be. This distinction is important because learning should remain a space for development rather than continuous judgement (Prinsloo & Slade, 2017; Slade & Prinsloo, 2013).

5.4 Purpose limitation

Purpose limitation protects employees from function creep. Data collected for learning should not automatically become data for discipline, promotion, termination, or workforce reduction. Any secondary use should be clearly defined, justified, communicated, and reviewed (European Parliament and Council of the European Union, 2016). Organisations should create data firewalls between developmental learning analytics and employment decision-making. This does not mean learning data can never inform workforce planning. Rather, it means that the use of such data must be controlled, transparent, proportionate, and fair. Individual-level developmental data should be protected more strongly than aggregated programme data (Khan & Tang, 2016; Tursunbayeva et al.,

DOI: https://doi.org/10.5281/zenodo.20639001

2021). Purpose limitation also requires retention control. Learning data should not be stored indefinitely simply because storage is cheap. Old learning errors should not follow employees permanently. Retention schedules should reflect the purpose of the data. This is especially important because long-term storage can convert temporary learning struggles into permanent reputational risks (Moore, 2020; O'Neil, 2016).

5.5 Employee agency

Employee agency means that employees are treated as active participants in data governance, not passive data sources. Employees should have rights to access, correct, understand, contest, and, where appropriate, delete or restrict the use of their learning data (European Parliament and Council of the European Union, 2016). Agency also includes a collective voice. Employees and their representatives should be consulted before AI-enabled learning platforms are introduced. Consultation can identify risks that managers or vendors may overlook. It can also improve trust and legitimacy. Worker participation is particularly important where AI systems affect opportunity, evaluation, and workplace power relations (Kellogg et al., 2020; Moore, 2020). Employee agency also requires contestability. Employees should not be trapped inside algorithmic classifications. If an AI system labels an employee as low engagement, low skill, or high risk, the employee should be able to understand the basis of that classification and challenge it. This is essential to procedural fairness and personal dignity (Binns, 2022; Martin, 2019).

5.6 Accountable governance

Accountable governance requires clear responsibility for AI data practices. Organisations should not treat AI-enabled learning as merely an HR or IT procurement issue. It should be governed through cross-functional oversight involving learning and development, HR, legal, privacy, information security, ethics, employee representatives, and senior leadership (Floridi & Cowls, 2022; OECD, 2019). Accountability mechanisms should include data protection impact assessments, algorithmic impact assessments, bias audits, vendor due diligence, explainability requirements, human review procedures, employee complaint channels, audit trails, retention reviews, and governance reporting. These mechanisms are necessary because AI systems can create harm even when no individual manager intends harm (Leicht-Deobald et al., 2019; Martin, 2019). Where AI outputs affect employment opportunities, human oversight must be meaningful. A human manager should not simply approve algorithmic recommendations without understanding them. Human review should involve critical evaluation, contextual judgement, and openness to employee challenge (Binns, 2022; European Parliament and Council of the European Union, 2024).

6. Discussion

The ethical boundaries of AI data collection in workplace learning are shaped by a fundamental tension between development and control. On one hand, organisations have legitimate interests in improving employee skills, ensuring compliance, and preparing for technological change. On the other hand, employees have legitimate interests in privacy, autonomy, dignity, fairness, and protection from excessive surveillance (Ball, 2021; Floridi & Cowls, 2022). This paper argues that workplace learning platforms should be understood as socio-technical governance systems. They are not neutral tools. Their design choices shape what counts as learning, what counts as engagement, what becomes visible to management, and how employees are classified (Williamson, 2017). Metrics are not merely descriptive; they can become normative. They define what the organisation values and what employees feel pressured to perform (Lyon, 2018; Zuboff, 2019). The concept of the digital employee helps explain this transformation. The digital employee is produced through data collection, profiling, prediction, and managerial interpretation. In AI-enabled learning platforms, the digital employee may appear as a skills map, engagement score, readiness index, or risk profile. These representations can support development, but they can also reduce employees to simplified data objects (Ajunwa, 2020; Moore, 2020). The most important ethical boundary is the boundary between learning support and employment surveillance.

DOI: https://doi.org/10.5281/zenodo.20639001

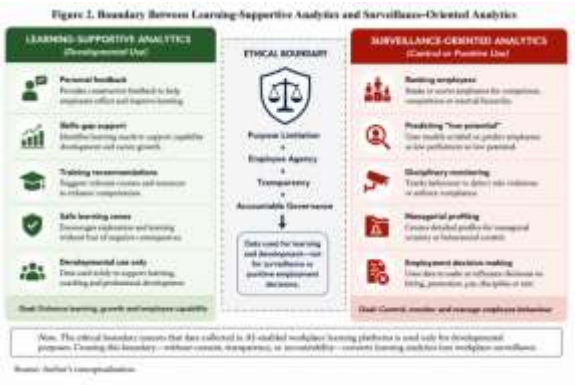

Figure 2 illustrates the ethical boundary between learning-supportive analytics and surveillance-oriented analytics. It shows that AI-generated learning data should be used primarily for employee development, feedback, and capability building, rather than for punitive monitoring, ranking, or employment decision-making.

Learning-supportive analytics are designed to help employees grow. They provide feedback, recommend resources, identify support needs, and improve training design. Surveillance-oriented analytics are designed to monitor, compare, rank, discipline, or control employees (Kellogg et al., 2020; Sánchez-Monedero & Dencik, 2022). The same data can serve either purpose depending on governance. For example, an assessment score can help an employee identify areas for improvement, or it can be used by a manager to judge incompetence. Ethical governance must protect the developmental purpose of learning data.

Another key argument is that consent cannot carry the full ethical burden. In employment contexts, employees may not have genuine freedom to refuse. Therefore, organisations must rely on more robust safeguards: minimisation, purpose limitation, proportionality, privacy by design, consultation, and accountability (European Data Protection Board, 2020; European Parliament and Council of the European Union, 2016). Consent should be treated as one element of ethical governance, not as a blanket permission slip. Trust is also central. Workplace learning depends on trust because employees must be willing to expose what they do not know. If employees believe that AI learning platforms are hidden surveillance systems, they may resist, disengage, or manipulate metrics. Ethical data governance is therefore not only a rights issue but also a practical condition for effective learning (Prinsloo & Slade, 2017; Slade & Prinsloo, 2013).

7. Practical Recommendations

7.1 Recommendations for organisations

Organisations should begin by mapping all data collected by workplace learning platforms. This map should identify raw data, derived data, inferred data, access rights, retention periods, vendor processing, and employment uses. Many organisations cannot govern ethically because they do not fully understand their own data flows (Tursunbayeva et al., 2021). Second, organisations should conduct data protection and algorithmic impact assessments before deployment. These assessments should examine necessity, proportionality, bias, explainability, security, and employee consequences. They should not be treated as paperwork exercises (European Parliament and Council of the European Union, 2016, 2024). Third, organisations should separate developmental analytics from disciplinary processes. Employees should know which data is used only for learning and which data may affect employment decisions. Sensitive learning data should not be casually shared with line managers (Ball, 2021; Moore, 2020). Fourth, organisations should provide employees with meaningful explanations. Employees should understand how recommendations, scores, classifications, and alerts are generated. Explanations should be practical rather than purely technical (Binns, 2022; Martin, 2019). Fifth, organisations should provide rights of access, correction, contestation, and human review. Employees should be able to challenge inaccurate learning profiles or algorithmic conclusions (European Parliament and Council of the European Union, 2016; Leicht-Deobald et al., 2019). Sixth, organisations should consult employees before introducing AI-enabled learning platforms. Consultation should occur early, before procurement and deployment decisions are final. This approach supports legitimacy and reduces the risk that AI adoption will be experienced as imposed surveillance (Kellogg et al., 2020; Moore, 2020).

7.2.Recommendations for platform developers

DOI: https://doi.org/10.5281/zenodo.20639001

Platform developers should design systems that support privacy, transparency, and employee agency by default. They should avoid dark patterns that pressure employees into unnecessary data sharing. They should provide configurable privacy settings, clear analytics explanations, and role-based access controls (Floridi & Cowls, 2022; OECD, 2019). Developers should avoid intrusive data collection unless strictly necessary. Biometric and affective analytics should not be included as default features in workplace learning platforms. Where such features exist, they should require explicit justification and strong safeguards (Crawford, 2021; Moore, 2020).

Developers should also support auditability. Organisations should be able to examine how AI models generate recommendations, what data is used, and whether outputs differ across groups. Without auditability, organisations cannot responsibly govern workplace AI systems (Köchling & Wehner, 2020; Martin, 2019).

7.3 Recommendations for policymakers and regulators

Policymakers should provide clearer guidance on AI-enabled workplace learning and employee data. Existing data protection and employment laws may apply, but organisations need practical standards for learning analytics, consent, secondary use, and algorithmic profiling (European Data Protection Board, 2020; European Parliament and Council of the European Union, 2024). Regulators should pay special attention to systems that connect learning data with employment decisions. Where AI learning analytics affect promotion, discipline, redundancy, or access to opportunity, stronger transparency and contestation rights are needed (Ajunwa, 2020; Binns, 2022). Regulators should also encourage worker consultation. AI governance should not be limited to technical compliance; it should include democratic participation in workplace technology decisions. This is particularly important because workplace AI can reshape power relations even when it is introduced under the language of innovation and efficiency (Kellogg et al., 2020; Newlands, 2021).

8. Conclusion

AI-enabled workplace learning platforms are reshaping how organisations train, evaluate, and understand employees. These systems can supportpersonalisation, reskilling, compliance, and organisational learning. However, they also intensify data collection and create new risks of surveillance, profiling, coercive consent, function creep, bias, and loss of employee agency (Ball, 2021; Moore, 2020; Zuboff, 2019). This paper has argued that the ethical boundaries of AI data collection in workplace learning must be grounded in the realities of the employment relationship. Employees often cannot provide fully voluntary consent because of organisational hierarchy and dependency. Privacy risks are not limited to data breaches; they include intrusive inference, behavioural control, and unfair employment consequences (European Data Protection Board, 2020; European Parliament and Council of the European Union, 2016). Learning data is ethically sensitive because it captures vulnerability, error, development, and potential.

The proposed Ethical Boundary Framework offers six principles for responsible governance: contextual consent, privacy by design, proportionality, purpose limitation, employee agency, and accountable governance.

These principles require organisations to treat workplace learning platforms not as neutral technologies but as systems of power that must be governed carefully. The future of workplace learning should not be based on invisible surveillance or unrestricted data extraction. It should be based on responsible data stewardship.AI can support human development only when it respects human dignity. Organisations that protect consent, privacy, and employee agency are more likely to build learning cultures based on trust, fairness, and sustainable innovation.

References

Ajunwa, I. (2020). The paradox of automation as anti-bias intervention. *Cardozo Law Review, 41*(5), 1671–1742.

Ball, K. (2021). Electronic monitoring and surveillance in the workplace. *European Foundation for the Improvement of Living and Working Conditions*.

Binns, R. (2022). Human judgment in algorithmic loops: Individual justice and

DOI: https://doi.org/10.5281/zenodo.20639001

automated decision-making. *Regulation & Governance, 16*(1), 197–211.

Crawford, K. (2021). *Atlas of AI: Power, politics, and the planetary costs of artificial intelligence*. Yale University Press.

Dencik, L., Hintz, A., Redden, J., & Treré, E. (2019). Exploring data justice: Conceptions, applications and directions. *Information, Communication & Society, 22*(7), 873–881.

European Data Protection Board. (2020). *Guidelines 05/2020 on consent under Regulation 2016/679*. European Data Protection Board.

European Parliament and Council of the European Union. (2016). *Regulation EU 2016/679: General Data Protection Regulation*. Official Journal of the European Union.

European Parliament and Council of the European Union. (2024). *Regulation EU 2024/1689 laying down harmonised rules on artificial intelligence*. Official Journal of the European Union.

Floridi, L., & Cowls, J. (2022). A unified framework of five principles for AI in society. *Harvard Data Science Review, 1*(1), 1–15.
FRA. (2020). *Getting the future right: Artificial intelligence and fundamental rights*. European Union Agency for Fundamental Rights.

Ifenthaler, D., & Yau, J. Y. K. (2020). Utilising learning analytics to support study success in higher education: A systematic review. *Educational Technology Research and Development, 68*, 1961–1990.

Kellogg, K. C., Valentine, M. A., & Christin, A. (2020). Algorithms at work: The new contested terrain of control. *Academy of Management Annals, 14*(1), 366–410.
Khan, S., & Tang, J. (2016). The paradox of human resource analytics: Being mindful of employees. *Journal of General Management, 42*(2), 57–66.

Köchling, A., & Wehner, M. C. (2020). Discriminated by an algorithm: A systematic review of discrimination and fairness by algorithmic decision-making in the context of HR recruitment and HR development. *Business Research, 13*, 795–848.

Leicht-Deobald, U., Busch, T., Schank, C., Weibel, A., Schafheitle, S., Wildhaber, I., & Kasper, G. (2019). The challenges of algorithm-based HR decision-making for personal integrity. *Journal of Business Ethics, 160*, 377–392.

Lyon, D. (2018). *The culture of surveillance: Watching as a way of life*. Polity Press.
Martin, K. (2019). Ethical implications and accountability of algorithms. *Journal of Business Ethics, 160*, 835–850.

Moore, P. V. (2020). Data subjects, digital surveillance, AI and the future of work. *European Labour Law Journal, 11*(1), 45–59.
Newlands, G. (2021). Algorithmic surveillance in the gig economy: The organization of work through Lefebvrian conceived space. *Organization Studies, 42*(5), 719–737.

OECD. (2019). *OECD principles on artificial intelligence*. Organisation for Economic Co-operation and Development.

OECD. (2023). *The impact of AI on the workplace: Main findings from the OECD AI surveys of employers and workers*. OECD Publishing.

O'Neil, C. (2016). *Weapons of math destruction: How big data increases inequality and threatens democracy*. Crown.
Ponce Del Castillo, A. (2021). The AI regulation: Entering an AI regulatory winter? *European Trade Union Institute Working Paper*.

Prinsloo, P., & Slade, S. (2017). An elephant in the learning analytics room: The obligation to act. *Proceedings of the Seventh International Learning Analytics & Knowledge Conference*, 46–55.

Sánchez-Monedero, J., & Dencik, L. (2022). The datafication of workplace surveillance and worker resistance. *Big Data & Society, 9*(2), 1–13.

DOI: https://doi.org/10.5281/zenodo.20639001

Selwyn, N. (2019). *Should robots replace teachers? AI and the future of education*. Polity Press.

Slade, S., & Prinsloo, P. (2013). Learning analytics: Ethical issues and dilemmas. *American Behavioral Scientist, 57*(10), 1510–1529.

Tsamados, A., Aggarwal, N., Cowls, J., Morley, J., Roberts, H., Taddeo, M., & Floridi, L. (2022). The ethics of algorithms: Key problems and solutions. *AI & Society, 37*, 215–230.

Tursunbayeva, A., Pagliari, C., Di Lauro, S., & Antonelli, G. (2021). The ethics of people analytics: Risks, opportunities and recommendations. *Personnel Review, 50*(3), 900–921.

West, S. M., Whittaker, M., & Crawford, K. (2019). *Discriminating systems: Gender, race and power in AI*. AI Now Institute.

Williamson, B. (2017). *Big data in education: The digital future of learning, policy and practice*. SAGE.

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. PublicAffairs.

DOI: https://doi.org/10.5281/zenodo.20639001