

Algorithmic Decision-Making in Employment: Legal Challenges of Artificial Intelligence in Recruitment and Workplace Management

Dr. Anushka Perera¹, Prof. Neeraj Iyer¹

¹ Centre for Labour Law and Emerging Technologies, Sri Lanka Institute of Legal Studies, Kandy, Sri Lanka

² Department of Technology Law and Digital Security, Indian Institute of Legal Technology, Hyderabad, India.

Received: 18 Nov 2025 **Revised:** 28 Feb 2026 **Accepted:** 28 April 2025 **Published:** 24 June 2026

ABSTRACT

Artificial intelligence is increasingly being used by organizations to automate recruitment, employee assessment, performance evaluation, workforce management, and promotion-related decisions. Algorithmic decision-making can improve organizational efficiency by processing large quantities of information and identifying patterns that may not be immediately visible to human decision-makers. However, the use of AI in employment environments also creates significant legal and technological concerns relating to discrimination, privacy, transparency, accountability, data protection, and human oversight. This article examines the technological foundations of AI-based employment decision-making and analyzes the principal legal challenges arising from its deployment in recruitment and workplace management. Particular attention is given to algorithmic bias, automated profiling, biometric monitoring, employee data, explainability, and responsibility for erroneous decisions. The article argues that efficiency and predictive accuracy alone cannot justify automated employment decisions where fundamental workplace rights may be affected. It proposes a human-centred governance framework based on transparency, data minimization, algorithmic auditing, explainability, human review, cybersecurity, and effective mechanisms for challenging automated decisions. The article concludes that AI can transform employment practices positively, but responsible deployment requires technological safeguards combined with appropriate legal and institutional accountability.

Keywords: Artificial Intelligence; Employment Law; Algorithmic Decision-Making; Recruitment Technology; Workplace Surveillance; Algorithmic Bias; Data Protection.

© 2026. The Author(s). This is an open-access article distributed under the terms of the Creative Commons Attribution 4.0 International License (CC BY 4.0), which permits unrestricted use, distribution and reproduction in any medium, provided the original work is properly cited.

1. Introduction

Artificial intelligence has rapidly entered the modern workplace. Organizations increasingly use AI-powered technologies to recruit employees, analyze applications, evaluate candidates, monitor productivity, predict employee performance, and support management decisions. Traditional recruitment generally involved human review of applications, interviews, professional references, and other information. AI systems can now analyze thousands of applications within a relatively short period and rank candidates according to predefined criteria.

Similarly, workplace-management technologies can analyze employee activity, communication patterns, attendance, productivity indicators, and other forms of digital information.

These technologies may significantly improve organizational efficiency. However, employment decisions have direct consequences for individuals' professional lives and economic opportunities.

An algorithmic system that incorrectly rejects a qualified candidate or produces a biased employee assessment may cause substantial harm.

The legal challenge is therefore to determine how AI can be used to improve employment processes without undermining fairness, privacy, equality, and accountability.

This article examines the technological and legal dimensions of algorithmic decision-making in employment and proposes a framework for responsible implementation.

2. AI-Based Recruitment

AI-based recruitment systems can perform a variety of tasks.

These may include:

- filtering applications;
- ranking candidates;
- analyzing resumes;
- matching qualifications with job descriptions;
- scheduling interviews;
- conducting automated assessments; and
- generating candidate recommendations.

Such systems can reduce administrative workloads, particularly for organizations receiving large numbers of applications.

However, automated recruitment systems depend upon the data and criteria used to develop them.

If historical recruitment data contains patterns of discrimination or organizational bias, an AI system may reproduce those patterns.

Consequently, automation does not necessarily eliminate human bias. It may simply transform human bias into algorithmic form.

3. Algorithmic Bias

Algorithmic bias is one of the most important challenges associated with AI-based employment decisions.

Bias can arise when training datasets are incomplete, unrepresentative, or historically biased.

For example, if a recruitment model is trained using historical hiring decisions that disproportionately favored a particular category of applicants, the system may learn that pattern.

Bias can also result from seemingly neutral variables that indirectly correlate with protected characteristics.

Therefore, organizations should not assume that an algorithm is objective simply because it is mathematical.

Regular testing should be conducted to identify whether the system produces materially different outcomes among relevant groups.

4. Automated Profiling

AI systems can create detailed profiles of applicants and employees.

These profiles may include information concerning qualifications, professional history, behavioral characteristics, productivity, communication patterns, or other digital indicators.

The collection and analysis of such information raises important privacy questions.

Organizations should identify the legitimate purpose for collecting employee information and avoid excessive processing unrelated to that purpose.

The more information an organization collects, the greater the potential consequences of unauthorized access or misuse.

5. Employee Privacy

AI-powered workplace systems can potentially monitor employees continuously.

Examples include software that analyzes:

- computer activity;
- email usage;
- workplace communications;
- location;
- attendance;
- keystrokes;
- productivity indicators; and
- access to organizational systems.

Although monitoring may serve legitimate security or operational purposes, excessive surveillance can undermine employee privacy and autonomy.

Organizations should therefore establish clear boundaries regarding what information may be collected and how it may be used.

6. AI-Based Performance Evaluation

Organizations may use AI to evaluate employee performance.

An algorithm might analyze productivity indicators and generate a performance score.

While such systems can provide useful analytical information, performance is often multidimensional.

A numerical score may fail to capture creativity, teamwork, leadership, problem-solving ability, or other qualitative characteristics.

Overreliance on automated scores may therefore result in unfair evaluations.

AI should generally support managerial judgment rather than completely replace it.

7. Transparency and Explainability

Employees and applicants may not know when AI has influenced a decision concerning them.

This creates a transparency problem.

If an applicant is rejected because an algorithm assigned a low suitability score, the individual may have difficulty understanding why.

Explainability is therefore particularly important when automated systems have significant consequences.

Organizations should be capable of explaining, at an appropriate level, the purpose of the system, the types of information considered, and the role played by automated analysis.

8. Human Oversight

Human oversight is an essential safeguard against algorithmic errors.

An AI system may provide a recommendation, but an appropriately qualified human decision-maker should have the ability to review the relevant circumstances.

Human review is particularly important where decisions involve:

- hiring;
- termination;
- promotion;
- disciplinary action;

- compensation; or
- significant changes in employment conditions.

Human oversight should be meaningful rather than merely procedural.

A manager should be able to question and reject an algorithmic recommendation when evidence suggests that it is inappropriate.

9. Biometric Technologies in the Workplace

Some organizations are experimenting with biometric technologies such as facial recognition and voice analysis.

Potential applications include employee authentication, access control, and attendance management.

However, biometric information is closely associated with individual identity and therefore requires strong security.

Organizations should carefully evaluate whether biometric monitoring is genuinely necessary and whether less intrusive alternatives are available.

Biometric systems should also incorporate appropriate security controls to reduce the risk of unauthorized access.

10. AI and Workplace Surveillance

The increasing availability of workplace analytics has created new forms of employee surveillance.

AI can potentially analyze patterns of communication and activity at a scale that would be difficult for humans to achieve.

This raises the possibility of highly detailed employee monitoring.

From a technological perspective, continuous monitoring can produce large quantities of information.

From a legal and ethical perspective, however, organizations must consider whether the level of monitoring is proportionate to its purpose.

Efficiency should not automatically justify unlimited surveillance.

11. Cybersecurity Risks

AI employment systems contain valuable personal and organizational information.

A security breach could expose applicant records, employee profiles, salary information, professional histories, or other confidential information.

Organizations should therefore implement strong cybersecurity measures, including:

- encryption;
- access controls;
- multi-factor authentication;
- secure data storage;
- audit logging;
- vulnerability management; and
- incident-response procedures.

AI systems should also be regularly tested for security weaknesses.

12. Responsibility for Algorithmic Errors

An important question concerns who should be responsible when an AI employment system produces an incorrect or discriminatory outcome.

Possible actors include:

- the employer;
- AI software providers;

- system developers;
- data suppliers; and
- human decision-makers.

Responsibility should not simply be attributed to the algorithm.

An organization deploying AI remains responsible for understanding how the system operates and monitoring its performance.

Contracts with AI vendors should clearly define responsibilities concerning security, accuracy, data management, updates, and incident reporting.

13. AI Vendors and Third-Party Systems

Many organizations purchase AI recruitment systems from external technology providers.

This creates additional governance challenges because employers may not have complete knowledge of how proprietary algorithms operate.

A vendor may consider the model architecture or training methodology commercially confidential.

However, complete opacity can make meaningful accountability difficult.

Organizations should therefore conduct appropriate vendor due diligence before deploying high-impact AI systems.

Contracts should also include provisions concerning auditing, security, data protection, system performance, and vulnerability disclosure.

14. Data Quality

AI systems depend heavily on data quality.

Poor-quality data may include:

- inaccurate records;
- outdated information;
- missing values;
- inconsistent classifications; or
- unrepresentative samples.

If such data is used to make employment decisions, errors may become systematic.

Organizations should therefore establish procedures for data validation and quality control.

Data should also be periodically reviewed because workplace conditions and organizational requirements change over time.

15. AI and Employment Discrimination

AI can create both new forms of discrimination and new methods for identifying discrimination.

If properly designed, analytical systems may help organizations detect unequal outcomes.

However, biased algorithms can also produce discriminatory results.

Organizations should therefore evaluate systems not only for overall accuracy but also for differential outcomes.

Independent algorithmic audits may provide useful mechanisms for identifying potential problems.

16. Proposed Governance Framework

A responsible AI employment framework should include several elements.

16.1 Purpose Specification

Organizations should clearly define why an AI system is being deployed.

16.2 Data Minimization

Only information reasonably necessary for the stated purpose should be processed.

16.3 Bias Testing

Systems should be tested for discriminatory or materially unequal outcomes.

16.4 Explainability

Organizations should maintain appropriate explanations of how AI contributes to decisions.

16.5 Human Review

Significant employment decisions should include meaningful human oversight.

16.6 Security

Applicant and employee information should be protected through appropriate technical measures.

16.7 Auditability

Organizations should maintain records sufficient to evaluate system performance and decision-making.

16.8 Challenge Mechanisms

Applicants and employees should have appropriate mechanisms for questioning significant automated decisions.

17. Privacy-by-Design Approach

Privacy should be incorporated into AI employment systems from the beginning.

A privacy-by-design architecture may include:

Data Collection Layer → collects only necessary information.

Processing Layer → performs authorized AI analysis.

Security Layer → protects information through encryption and access controls.

Decision Layer → generates recommendations rather than automatically determining outcomes.

Human Review Layer → allows qualified personnel to evaluate significant decisions.

Audit Layer → records system activity and decision processes.

This architecture can reduce unnecessary data exposure while preserving the benefits of automation.

18. AI and Remote Work

The expansion of remote work has increased interest in digital monitoring technologies.

Organizations may use AI to analyze work activity, communication patterns, and task completion.

Such systems can potentially support workforce management, but excessive monitoring may create significant privacy concerns.

Remote employees should not automatically be treated as requiring continuous digital surveillance.

Organizations should distinguish between legitimate productivity management and disproportionate monitoring.

19. Future of AI in Employment

AI is likely to become increasingly integrated into employment systems.

Future applications may include sophisticated skills matching, personalized employee development, predictive workforce planning, automated training recommendations, and AI-supported organizational decision-making.

Generative AI may also assist with recruitment communication, job descriptions, employee training, and workplace documentation.

As these systems become more sophisticated, the distinction between technological assistance and automated decision-making may become increasingly important.

Regulatory frameworks should therefore focus on the potential impact of a system rather than merely its technical classification.

20. Conclusion

Artificial intelligence is transforming the modern workplace by changing how organizations recruit, evaluate, manage, and communicate with employees.

AI-based systems can improve efficiency, process large quantities of information, and support organizational decision-making. However, technological efficiency cannot by itself justify automated employment decisions.

Algorithmic bias, employee surveillance, privacy risks, inaccurate predictions, opaque decision-making, cybersecurity vulnerabilities, and unclear responsibility can create significant legal challenges.

A responsible approach should combine technological innovation with strong governance.

Purpose limitation, data minimization, algorithmic auditing, explainability, cybersecurity, human oversight, vendor accountability, and mechanisms for challenging significant decisions should form the foundation of AI-based employment systems.

The central principle should be that artificial intelligence assists employment decision-makers rather than becoming an unaccountable replacement for human judgment.

As AI becomes increasingly embedded in the workplace, organizations will need to treat algorithmic governance as an essential component of employment management. The future of AI-enabled employment should therefore be based not simply on what technology can do, but on what technology can responsibly and fairly do within a legally accountable workplace.

Declarations

Conflict of interest: The authors declare that they have no conflict of interest.

Funding: This review received no specific grant from any funding agency in the public, commercial or not-for-profit sectors.

Ethical approval: Not applicable. This article is a review of published literature and did not involve human participants or animal subjects.

Data availability: No new data were generated or analyzed in support of this review. All sources relied upon are cited in the References.

Use of AI tools: No generative artificial intelligence tool was used in the conception, drafting or analysis of this article. The authors take full responsibility for the content.

Author contributions: Author contributed to the conception of the review, the survey of the literature, and the drafting and revision of the manuscript. Author read and approved the final version.