International Journal of Social and Education (INJOSEDU) https://languar.net/index.php/INJOSEDU
Vol. 3 No. 2 May 2026, hal., 183-195 e-ISSN: 3047-6151

THE TRANSFORMATION OF HUMAN RESOURCE MANAGEMENT IN THE DIGITAL AGE: A LEGAL ANALYSIS OF THE PROTECTION OF EMPLOYEES' PERSONAL DATA AND COMPLIANCE WITH LABOUR REGULATIONS FOLLOWING THE 2022 PERSONAL DATA PROTECTION ACT

Gunawan Widjaja
Senior Lecturer, Faculty of Law Universitas 17 Agustus 1945 Jakarta
widjaja_gunawan@yahoo.com

Abstract

Digital transformation has revolutionised Human Resource Management (HRM) from an administrative function into a data-driven strategic ecosystem utilising artificial intelligence, predictive analytics, and integrated systems. However, the adoption of this technology poses serious legal challenges regarding the protection of employees' personal data amidst the unequal power dynamics between employers and employees. This study aims to analyse digital transformation in HRM and the legal implications of Law No. 27 of 2022 on Personal Data Protection (PDP Law) for compliance with labour regulations in Indonesia. It employs a literature review (*library research*) using a legal-normative approach. The research findings indicate that digital transformation in HRM—encompassing AI-based recruitment, HRIS, digital monitoring, and biometrics—has enhanced efficiency whilst simultaneously creating massive privacy risks for workers. The 2022 PDP Act reshapes the labour law landscape by designating employers as Data Controllers who must adhere to the principles of purpose limitation, multi-layered data security, transparency, and structural accountability. This regulation curtails employers' prerogatives through a proportionality test and strengthens workers' rights to access, rectification, erasure, and data portability. Compliance with the 2022 PDP Act demands a fundamental overhaul of HR policies, investment in cybersecurity, the appointment of a Data Protection Officer (DPO), and the implementation of *Privacy by Design*. This study concludes that the success of digital transformation in HRM is not only measured by operational efficiency, but by the organisation's ability to integrate technological innovation with the protection of workers' human rights, thereby realising a fair, safe, and legally certain working ecosystem in the digital economy era.

Keywords: digital transformation, human resource management, personal data protection, Personal Data Protection Act 2022, labour compliance, worker privacy, labour law.

Introduction

The Fourth Industrial Revolution and Society 5.0 have driven the acceleration of digital transformation across various sectors, including human resource management (HRM), which is now shifting from conventional administrative approaches towards data-driven and artificial intelligence (AI)-based ecosystems. This digitalisation enables organisations to optimise operational efficiency, improve decision-making accuracy, and create a more personalised work experience for employees through the use of *Human Resource Information Systems* (HRIS) and *big data* analytics (Glavin et al., 2024) . However,

behind this efficiency lie new complexities regarding the privacy and security of employees' personal information, which constitutes the most crucial asset in the digital economy.

HRM transformation in the digital era is characterised by the adoption of advanced technologies such as *cloud computing*, *the Internet of Things* (IoT), and *machine learning* algorithms, which facilitate processes ranging from recruitment and performance appraisal to career development in *real-time*. The use of these tools enables companies to collect, store, and process employees' personal data in massive volumes and diverse forms, ranging from biometric data and health records to digital behaviour patterns in the workplace (Wu & Kao, 2022) . This phenomenon creates a paradox where managerial efficiency is directly proportional to an increased risk of privacy breaches if not managed with strict governance.

Indonesia, as the largest digital economy in Southeast Asia, has seen a significant surge in the adoption of HRM technology, particularly following the COVID-19 pandemic, which forced the acceleration of *remote* and hybrid *working*. Surveys indicate that over 70% of companies in Indonesia have implemented digital systems to manage employee data; however, the majority do not yet have adequate cybersecurity protocols to protect such sensitive data from the threat of leaks or misuse (Anwar & Nurrohman, 2025) . This gap between technology adoption and data governance maturity creates a serious legal vulnerability for both workers and employers.

Workers' personal data in the context of industrial relations has unique characteristics due to the unequal power dynamic between employers and workers, which has the potential to trigger data exploitation for the company's unilateral interests. Practices such as *digital surveillance*, *real-time* location tracking, and predictive analysis of employee performance are often carried out without transparency or valid consent from the data subjects (Aloisi, 2015) . This raises fundamental questions regarding the limits of employers' prerogative in managing business operations and workers' fundamental rights to privacy and the protection of personal data.

Prior to 2022, personal data protection in Indonesia was fragmented across various sectoral regulations such as the ITE Law, the Labour Law, and the Minister of Communication and Information Technology Regulation, creating legal fragmentation and uncertainty in enforcement. The absence of a comprehensive umbrella *law* has led to varying standards of worker data protection across sectors, which are often out of step with international data protection principles such as *purpose limitation* and *data minimisation* (Versaci, 2018) . This situation is exacerbated by the lack of stringent sanctions for offenders, leading many companies to neglect privacy compliance aspects within their digital HR systems.

A turning point in the legal landscape occurred with the enactment of Law No. 27 of 2022 on Personal Data Protection (PDP Law), which marks a new era in Indonesia's privacy legal regime and adopts global standards similar to the European Union's *General Data Protection Regulation* (GDPR). This Act establishes the fundamental principles of data

processing, the rights of data subjects, the obligations of data controllers and processors, as well as strict administrative and criminal sanction mechanisms for violators (Government of the Republic of Indonesia, 2022). For the world of employment, the 2022 PDP Law serves as the primary legal foundation requiring companies to revise all policies and procedures for managing employee data to comply with this new legal mandate.

The implementation of the 2022 Personal Data Protection Act within the context of HRM demands transformation not only in technological aspects but also in organisational culture and *a culture of* legal *compliance* within the company. Employers now hold the status of Data Controllers and are obliged to ensure that all processing of employee data is based on a valid legal basis, has a specific purpose, and is carried out with adequate security measures (Xiaying, 2019) . Failure to meet these obligations not only risks incurring fines of up to 2% of the company's annual turnover, but also damages the organisation's reputation in the eyes of the public and investors.

On the other hand, the harmonisation of the 2022 Personal Data Protection Act with existing labour regulations, such as Law No. 13 of 2003 on Labour and Law No. 6 of 2023 on Job Creation, still presents challenges regarding interpretation and implementation in practice. There is a potential conflict of norms regarding employers' authority to access workers' data for disciplinary purposes versus workers' rights to refuse the processing of irrelevant data (Hermawan, 2024) . This ambiguity requires in-depth legal analysis to formulate clear boundaries so that legal certainty can be established for both parties in industrial relations.

The phenomenon of personal data breaches in the employment sector is becoming increasingly concerning, in line with the rise in cyberattacks and internal data leaks involving the sensitive information of millions of Indonesian workers. Cases such as the BPJS Ketenagakerjaan data breach and the misuse of job applicants' data by illegal *job portal* platforms highlight the urgency of strengthening data protection mechanisms within the digital HRM ecosystem (Yudha et al., 2025) . Without a robust compliance framework, digital transformation could backfire, harming workers and hindering national productivity.

An analysis of compliance with labour regulations following the 2022 Personal Data Protection Act (PDP Act) is crucial to identifying the gap between legal norms (*das sollen*) and on-the-ground practices (*das sein*), as well as formulating risk mitigation strategies for companies. Companies need to conduct a comprehensive compliance audit, appoint a Data Protection Officer (*DPO*), and establish effective incident response mechanisms to fulfil the mandates of the Personal Data Protection Act (PDP Act) (Ventura & Coeli, 2018) . These proactive steps are not merely legal obligations, but strategic investments in building trust within sustainable industrial relations.

This article aims to critically analyse the transformation of human resource management in the digital age through the lens of personal data protection law, with a specific focus on the legal implications of the 2022 Personal Data Protection Act (PDP Act) for compliance with labour regulations.

Research Method

This study employs a literature review (*library research*) using a legal-normative approach to analyse the transformation of human resource management in the digital age, as well as the legal implications of the 2022 Personal Data Protection Act (PDP Act) on the protection of employees' personal data. Data collection was conducted through documentary study by examining primary legal sources, namely Law No. 27 of 2022 on Personal Data Protection, Law No. 13 of 2003 on Labour, Law No. 6 of 2023 on Job Creation, and related implementing regulations; secondary legal sources include national and international journals, books, and other documents discussing digital HR, data privacy, and labour law; as well as tertiary legal sources such as legal dictionaries and encyclopaedias to clarify key terminology. The collected data was then analysed qualitatively using content *analysis* and systematic interpretation to identify normative gaps, regulatory conflicts, and relevant legal principles, thereby enabling the formulation of coherent conclusions regarding compliance levels and strategic recommendations for stakeholders within the digital HRM ecosystem (McConville, 2017) ; (Eliyah & Aslan, 2025) .

Discussion

Digital Transformation in Human Resource Management

Digital transformation in Human Resource Management (HRM) is not merely the adoption of new technological tools, but a fundamental paradigm shift from administrative-bureaucratic functions towards a data-driven strategic role that integrates *Artificial Intelligence* (*AI*) and predictive analytics into every stage of the employee lifecycle. This evolution transforms the HR department from *a cost centre* into a *value creator* capable of providing strategic *insights* for executive decision-making through the use of advanced *People Analytics*. In this context, data is not merely a static archive, but a strategic asset which, if managed correctly, can predict *turnover* trends, identify skills gaps, and optimise talent allocation in real-time to support the organisation's business objectives (Glavin et al., 2024) .

One of the most tangible manifestations of this transformation is the digitalisation of recruitment and selection processes (*e-recruitment*), which now utilises *Machine Learning* algorithms to screen thousands of applicants in a matter of seconds, analyse keyword matches, and assess candidates' personalities through video analysis and facial micro-expressions. Platforms such as LinkedIn Talent Solutions, HireVue, and various AI-based *Applicant Tracking Systems* (ATS) enable companies to reduce human bias (though not entirely eliminate it), accelerate *time-to-hire*, and access the global talent market without geographical constraints. However, this efficiency brings new risks where unaudited algorithms may perpetuate historical biases embedded in training data, thereby potentially discriminating against certain groups systematically and violating the principle of equal employment opportunities (De Stefano, 2018) .

In addition to recruitment, the implementation of integrated *cloud-based Human Resource Information Systems* (HRIS) such as Workday, SAP SuccessFactors and Oracle HCM has revolutionised the way companies manage administrative data, attendance, payroll and employee benefits centrally and *in real time*. These systems enable self-service access for employees to update personal data, request leave, and access payslips via mobile devices, which significantly enhances *the employee experience* and reduces the administrative burden on HR staff. Furthermore, the integration of HRIS with a company's financial and operational systems creates a holistic data ecosystem, enabling the analysis of correlations between HR investment and the organisation's financial performance, although this demands far stricter cybersecurity standards to prevent mass data breaches (Bondarouk et al., 2017) .

The digital era has also given rise to the concept of *HR Analytics* or *People Analytics,* which utilises *Big Data* to transform managerial intuition into evidence-based decision-making (*evidence-based management*). By aggregating data from various sources—ranging from individual performance, employee *engagement*, health data, to digital traces of collaboration—companies can build predictive models to anticipate key *turnover*, identify future leaders, and design personalised development interventions. For example, algorithms can analyse email and calendar communication patterns to detect signs of burnout before an employee submits their resignation, enabling proactive intervention by managers. However, this practice treads a fine line ethically as it has the potential to become a form of invasive surveillance that erodes workers' autonomy and privacy (Angrave et al., 2016) .

The widespread phenomenon of *remote* and hybrid work following the COVID-19 pandemic has accelerated the adoption of digital collaboration tools such as Zoom, Microsoft Teams, and Slack, which have simultaneously transformed the dynamics of traditional monitoring and performance management. Companies are now shifting from presence-based management towards outcome-based management; however, many organisations are implementing *employee monitoring software* such as Time Doctor, Hubstaff, or even *keystroke logging* and *screen capture* to ensure the productivity of remote workers. These *digital surveillance* practices, whilst justified by employers as efforts to maintain accountability, often create a toxic work environment, increase employee stress, and trigger legal disputes regarding privacy breaches and *the right to disconnect* (Glavin et al., 2024) .

The use of biometric technology in the workplace, such as fingerprint scanners, facial recognition, and iris scanning for attendance and security access, is becoming increasingly common as it is considered more accurate and difficult to manipulate than conventional ID cards. Biometric data is categorised as sensitive personal data that poses a high risk if leaked, as it is permanent and cannot be altered like a password. The implementation of this technology in Indonesia, particularly in the manufacturing and logistics sectors, is often carried out without the workers' explicit *informed consent*, but rather as an absolute requirement for employment, reflecting an imbalance of power and

a potential breach of the principle of voluntariness in the processing of personal data (Nasution, 2023) .

Digital transformation has also facilitated the emergence of flexible working models and *the Gig Economy*, which are managed entirely through digital platforms, where algorithms act as an 'invisible boss' that automatically regulates task allocation, performance assessment, and even termination of employment. *Gig* workers such as online ride-hailing drivers and food delivery couriers are in a vulnerable position due to the ambiguous nature of their employment relationships, where their personal data and work behaviour are intensively monitored by platforms without adequate social protection guarantees. Non-transparent algorithms for determining rates and incentives (*black box algorithms*) make it difficult for workers to understand the logic behind decisions affecting their income, raising new legal challenges regarding algorithmic transparency and *the right to explanation* (De Stefano, 2018) .

From an employee development perspective, *Virtual Reality* (VR) and *Augmented Reality* (AR) technologies are now being utilised to create immersive and realistic training simulations, enabling employees to practise technical skills or high-risk scenarios without physical danger. Furthermore, AI-based *Learning Management System* (LMS) platforms such as Coursera for Business and LinkedIn Learning provide personalised learning content recommendations tailored to individual skills gaps and career paths. This personalisation enhances training effectiveness, but also requires extensive data collection on employees' learning styles, comprehension speeds, and performance histories, which in turn raises issues regarding data ownership and restrictions on its use for purposes other than e development .

The impact of digital transformation on industrial relations is not limited to technical aspects; it is also reshaping the psychology of employment contracts and the mutual expectations between employers and employees. Millennial and Gen Z employees expect transparency, flexibility and a seamless work experience akin to that of digital consumers, forcing HR departments to adopt a *consumer-grade technology* approach in their internal services. However, these expectations often clash with the reality of increasingly stringent digital surveillance, creating a paradox where technology designed to empower employees instead becomes a tool of control that restricts their autonomy, potentially undermining organisational trust and commitment (Roemmich et al., 2023) .

Ethical challenges in digital HR transformation are becoming increasingly complex due to the potential for algorithmic discrimination, where AI systems trained on biased historical data can produce decisions that disadvantage minority groups, women, or older workers. A real-world example occurred with Amazon's AI recruitment tool, which was scrapped after it was found to discriminate against female applicants due to having been trained on historical data reflecting male dominance in the technology industry. This underscores that technology is not a value-neutral entity, but rather a reflection of existing social biases, thus requiring regular algorithmic audits and diversification of development teams to ensure fairness and accountability in AI-based decision-making (Binns, 2018) .

In addition to the issue of bias, digital transformation also poses significant cybersecurity risks, with the personal data of millions of employees becoming an easy target for hackers and cybercrime syndicates. *Ransomware* attacks, *phishing*, and internal data breaches (*insider threats*) can lead to the mass exposure of sensitive information such as National Identity Numbers (NIK), bank accounts, medical records, and performance evaluations, the impact of which can be long-term and damaging for victims. Companies that fail to protect this data not only face legal action and regulatory fines, but also a loss of public trust and brand reputation that is difficult to restore, making cybersecurity a strategic priority in the HRM transformation agenda (Yu & Zhao, 2019) .

In the context of globalisation, multinational companies operating across different jurisdictions must navigate the challenge of complying with diverse data protection regimes, such as the GDPR in Europe, the CCPA in California, and now Indonesia's Personal Data Protection Act (UU PDP), each with its own distinct standards and requirements. Harmonising global HR policies with local regulations is crucial to avoid legal conflicts, for example regarding *cross-border* data transfers from Indonesian branches to data centres abroad. Non-compliance with any of these legal regimes can trigger severe extraterritorial sanctions, thus requiring close coordination between HR, legal, and IT functions to design a globally compliant data architecture (Bradford, 2020) .

Digital transformation in HR also demands a shift in competencies for HR professionals themselves, who must now possess data *literacy*, a basic understanding of technology, and a strong awareness of privacy laws to effectively manage the digital ecosystem. The role of *the HR Business Partner* is evolving into that of *an HR Data Analyst* and *Digital Ethics Officer*, responsible for ensuring that the use of technology remains within ethical and legal boundaries. Investment in *upskilling* and *reskilling* HR teams has become a strategic imperative, as an inability to adapt to technological change could render the HR function irrelevant and replaceable by automation (Cappelli, 2025) .

Overall, digital transformation in Human Resource Management offers extraordinary opportunities to enhance the efficiency, objectivity, and strategic value of the HR function, yet simultaneously poses significant risks to workers' privacy, autonomy, and fairness. A balance between technological innovation and the protection of workers' rights cannot be achieved by relying solely on voluntary corporate ethics; rather, it requires a robust regulatory framework, transparency in algorithmic decision-making, and effective oversight mechanisms. This is where the urgency of a legal analysis of the 2022 Personal Data Protection Act becomes crucial to ensure that digital transformation does not sacrifice human dignity for the sake of efficiency alone, but rather realises an inclusive, safe, and fair working ecosystem in the digital economy era.

Legal Analysis of Workers' Personal Data Protection and Regulatory Compliance

The enactment of Law No. 27 of 2022 on Personal Data Protection (PDP Law) marks a new milestone in Indonesia's labour law landscape, bringing an end to a decade of regulatory fragmentation where workers' data protection was merely implied in limited

provisions of the Labour Law and the ITE Law. This Act adopts universal data protection principles aligned with the European Union's *General Data Protection Regulation* (GDPR), positioning employees' personal data as a fundamental right that must be strictly protected, rather than merely a corporate administrative asset. For HR departments, this law changes the legal status of employers from mere record-keepers to "Personal Data Controllers" who bear fiduciary responsibility for every bit of information held about their employees, with far more severe legal consequences in the event of negligence (Government of the Republic of Indonesia, 2022; (Xiaying, 2019) .

One of the fundamental pillars of the 2022 Personal Data Protection Act (PDP Act) that drastically alters recruitment and performance management practices is the principle of the "*lawful basis for processing*" set out in Article 20. In the context of employment relationships, companies can no longer arbitrarily collect data on prospective or permanent employees based solely on the vague grounds of "business interests"; data processing must be based on explicit *consent*, the fulfilment of an employment contract, a legal obligation, or the vital interests of the data subject. This challenges common practice where job application forms often contain overly broad consent clauses (*blanket consent*) requiring applicants to grant access to social media, family health data, and even credit history—all of which have no direct relevance to job qualifications—which are now potentially void as they violate the principles of specificity and purpose limitation (Afifah, 2024) .

The categorisation of personal data under the 2022 Personal Data Protection Act (PDP Act) clearly distinguishes between general personal data and specific (sensitive) personal data, the latter of which includes health data, biometric data, genetic data, sexual life data, political views, criminal records, and data relating to children (Article 4). In HRM practice, this sensitive data is often collected unavoidably, ranging from pre-employment *medical check-up* (MCU) results, fingerprint data for attendance, to trade union membership information. The PDP Act requires stricter security measures and prohibits the processing of sensitive data unless very limited conditions are met, such as for health protection or the fulfilment of legal employment obligations, which compels companies to conduct in-depth audits of the types of data they hold and to delete data that lacks a clear legal basis (Hermawan, 2024) .

The data subject rights guaranteed in Chapter V of the 2022 Personal Data Protection Act grant workers new powers to control their personal information, including the right to access, rectify, erase (*right to erasure*), and restrict the processing of their data. Within the dynamics of an unequal industrial relationship, these rights serve as a crucial *check-and-balance* mechanism; a worker can now legally request that a company delete their biometric data following the termination of their employment, or refuse the processing of GPS location data outside working hours. A company's failure to facilitate these rights within the specified timeframe (a maximum of 3x24 hours for urgent requests) constitutes an administrative offence subject to progressive sanctions, ranging from a written warning to significant financial fines (Hermawan, 2024) .

The obligations of Personal Data Controllers (companies), as stipulated in Chapter VI of the 2022 Personal Data Protection Act, require structural transformation in human resources management, including the obligation to appoint a *Data Protection* Officer (DPO) for entities processing data on a large scale or for high-risk purposes. The DPO acts as an internal compliance bridge, ensuring that recruitment policies, employee data storage, and digital monitoring systems are aligned with the legal mandate. Furthermore, companies are required to develop and implement a personal data protection plan, conduct periodic evaluations, and maintain *a record of processing activities* (ROPA), which represents an accountability standard previously rarely applied in conventional HRM practices in Indonesia (Versaci, 2018) .

The data security provisions in the 2022 Personal Data Protection Act (Articles 26 and 43) set strict standards requiring Data Controllers to ensure the security of personal data through adequate technical and organisational measures, including encryption, anonymisation, and *role-based access control*. In the context of HRIS and *cloud computing*, this obligation becomes complex when employee data is stored on third-party servers or processed by external *payroll* vendors; the company remains fully liable for any data breaches occurring on the vendor's side, so *the Data Processing Agreement* (DPA) must be revised to clearly allocate risks and compensation obligations. Failure to implement these security standards, resulting in a data breach, is now subject to criminal penalties of up to five years' imprisonment and/or a fine of up to Rp5 billion for offenders under the Data Protection Act .

The most complex legal challenge following the 2022 Personal Data Protection Act is its harmonisation with Law No. 6 of 2023 on Job Creation and its implementing regulations, which still provide considerable scope for employers to regulate workplace discipline and supervision. There is a potential conflict of norms where employers' rights to monitor productivity (for example, through *screen recording* or email tracking) clash with workers' rights to privacy and the protection of personal data. Legal analysis indicates that employers' prerogative rights are no longer absolute; any form of digital monitoring must satisfy the proportionality test, have a legitimate purpose, and be conducted with full transparency towards workers, or risk being challenged as an unlawful act and a breach of the Personal Data Protection Act (De Stefano, 2018) .

The sanction mechanism under the 2022 PDP Act is designed using *a tiered approach*, encompassing administrative sanctions, civil damages, and criminal sanctions, creating *a deterrent effect* that is far stronger than previous regulations. Administrative sanctions may take the form of fines of up to 2% of annual *revenue* for corporations; a figure which, for multinational companies or technology *start-ups*, could reach trillions of rupiah, far exceeding the investment costs for compliance systems. Furthermore, this Act also paves the way for *class action* lawsuits by employees whose data has been leaked or misused, which has the potential to result in massive financial liability and permanent reputational damage for companies that breach the General Data Protection Regulation (GDPR) (Afifah, 2024) .

The issue of *cross-border data transfer* is highly relevant for multinational companies that centralise global HR data on overseas servers (for example, in Singapore or the United States). The 2022 Personal Data Protection Act (Article 56) stipulates that data transfers to other jurisdictions are only permitted if the destination country has a level of data protection equivalent to or higher than that of Indonesia, or if there is a bilateral/multilateral agreement, or if there are binding guarantees from the data recipient. This provision compels multinational companies to conduct *an adequacy assessment* of the destination country for the transfer and to draft compliant *Standard Contractual Clauses* (SCCs), or risk facing data flow blockages and legal sanctions in Indonesia (Bradford, 2020).

In compliance practice, many Indonesian companies remain trapped in a '*tick-box*' approach, where they merely update clauses in employment contracts without altering the substance of business processes or technological infrastructure. True compliance requires a *'Privacy by Design'* and *'Privacy by Default'* approach, where data protection principles are integrated from the design stage of HRIS systems, recruitment forms, right through to workplace monitoring policies. Companies need to conduct *a Data Protection Impact Assessment* (DPIA) before implementing new technologies such as AI recruitment or biometric systems, to identify and mitigate privacy risks before a breach occurs (Nasution, 2023) .

The role of trade unions and employee representative bodies is becoming increasingly strategic within the 2022 Personal Data Protection Act (PDP Act) ecosystem as internal oversight partners to ensure corporate data policies do not harm members. Trade unions can utilise the mandate of the PDP Act to demand algorithmic transparency in performance assessment systems, reject the processing of irrelevant sensitive data, and represent members in data breach disputes. This collaboration between HR functions, legal departments, and trade unions is essential for creating an inclusive culture of compliance, where data protection is viewed as a collective right of workers, not merely a regulatory obligation for companies (De Stefano, 2023; Aloisi, 2020).

A comparative study with other jurisdictions shows that the implementation of the Personal Data Protection Act (PDPA) in Indonesia still faces challenges regarding enforcement capacity and legal awareness amongst small and medium-sized enterprises (SMEs). Whilst large corporations are beginning to invest in Data Protection Officers (DPOs) and compliance systems, many SMEs still view the PDPA as a bureaucratic burden without fully understanding the existential risks posed by fines and legal action. The newly established data protection authority (Personal Data Protection Agency) faces the daunting task of conducting effective outreach, supervision and enforcement across the entire industrial spectrum; this requires a transition period and a phased approach to avoid stifling the business climate whilst still ensuring the protection of workers' rights (Hermawan, 2024) .

As a legal synthesis, the 2022 Personal Data Protection Act (PDP Act) is not merely a technical regulation on data protection, but an instrument for transforming industrial relations that shifts the balance of power from employer dominance towards a more

equitable partnership based on human rights. Compliance with this Act demands a fundamental reconstruction of HR policies, investment in cybersecurity technology, and a shift in organisational culture that places privacy as a core *value*. Companies that are able to adapt quickly will not only avoid legal and financial risks but also build a strong *employer brand* as an ethical and trustworthy organisation, which ultimately becomes a competitive advantage in the battle for talent in an increasingly privacy-conscious digital economy.

Conclusion

The transformation of Human Resource Management in the digital age has shifted the paradigm of workforce management from conventional administrative functions towards a data-driven strategic ecosystem powered by artificial intelligence, predictive analytics, and integrated systems. Whilst these innovations offer operational efficiency, objective decision-making, and a more personalised work experience, they simultaneously create serious vulnerabilities regarding employee privacy through practices of mass digital surveillance, the exploitation of sensitive data, and the potential for algorithmic discrimination. This dynamic underscores that technological advancements in HR cannot be separated from the urgency of protecting human rights in the workplace, where employees' personal data is not merely a corporate asset, but an extension of individual dignity that must be safeguarded against the abuse of unequal power dynamics.

The enactment of Law No. 27 of 2022 on Personal Data Protection (PDP Law) represents a crucial legal response that rebalances industrial relations by establishing strict standards for employers as Data Controllers. This regulation brings an end to the era of legal uncertainty by mandating the principles of purpose limitation, multi-layered data security, transparency of processing, and structural accountability through the appointment of a Data Protection Officer (DPO). Compliance with the 2022 PDP Act is no longer a voluntary option, but a legal imperative demanding deep harmonisation with existing labour regulations, where employers' prerogative to supervise and manage workers is now constrained by a proportionality test and workers' fundamental rights to privacy, access, rectification, and erasure of their personal data.

In conclusion, the success of digital transformation in HRM following the 2022 PDP Act is not measured solely by increased productivity or cost efficiency, but by an organisation's ability to integrate technological innovation with strong ethical principles and legal compliance. Companies that are able to adopt a '*Privacy by Design*' approach, build a culture of proactive compliance, and engage trade unions as oversight partners will achieve sustainable competitive advantage in the form of trust, a positive reputation, and better talent retention. Conversely, neglecting the mandate for personal data protection not only risks devastating administrative and criminal sanctions, but also erodes the foundations of fair, humane, and just industrial relations in the digital economy era.

References

Afifah, N. (2024). Tanggung Jawab Hukum Platform E-Commerce terhadap Keamanan Data Pribadi Pengguna: Analisis Berdasarkan UU PDP 2022. *Jurnal Legalitas*, *2*(1), 29–38. https://doi.org/10.58819/jle.v2i1.165

Aloisi, A. (2015). Commoditized workers: Case study research on labor law issues arising from a set of on-demand/gig economy platforms. *Comp. Lab. L. & Pol'y J.*, *37*, 653.

Angrave, D., Charlwood, A., Kirkpatrick, I., Lawrence, M., & Stuart, M. (2016). HR and analytics: Why HR is set to fail the big data challenge. *Human Resource Management Journal*, *26*(1), 1–11. https://doi.org/10.1111/1748-8583.12090

Anwar, K., & Nurrohman, R. (2025). Strategic HR Agility In Southeast Asian MSMES: A Cross-Country Study Of Indonesia, Vietnam, And The Philippines Amidst Digital Transformation. *JURNAL MANAJEMEN DAN BISNIS*, *4*(2), 432–452. https://doi.org/10.36490/jmdb.v4i2.1980

Binns, R. (2018). Fairness in Machine Learning: Lessons from Political Philosophy. *Proceedings of the 1st Conference on Fairness, Accountability and Transparency*, 149–159. https://proceedings.mlr.press/v81/binns18a.html

Bondarouk, T., Parry, E., & Furtmueller, E. (2017). Electronic HRM: Four decades of research on adoption and consequences. *The International Journal of Human Resource Management*, *28*(1), 98–131. https://doi.org/10.1080/09585192.2016.1245672

Bradford, A. (2020). *The Brussels Effect: How the European Union Rules the World*. Oxford University Press.

Cappelli, P. (2025). *The Future of the Office, with a New Afterword by the Author: Work from Home, Remote Work, and the Hard Choices We All Face*. University of Pennsylvania Press.

De Stefano, V. (2018). *'Negotiating the Algorithm': Automation, Artificial Intelligence and Labour Protection* (SSRN Scholarly Paper No. 3178233). Social Science Research Network. https://doi.org/10.2139/ssrn.3178233

Eliyah, E., & Aslan, A. (2025). STAKE'S EVALUATION MODEL: METODE PENELITIAN. *Prosiding Seminar Nasional Indonesia*, *3*(2), Article 2.

Fischer, F., Hmelo-Silver, C. E., Goldman, S. R., & Reimann, P. (2018). *International handbook of the learning sciences*. Routledge New York, NY. https://api.taylorfrancis.com/content/books/mono/download?identifierName=doi&identifierValue=10.4324/9781315617572&type=googlepdf

Glavin, P., Bierman, A., & Schieman, S. (2024). Private Eyes, They See Your Every Move: Workplace Surveillance and Worker Well-Being. *Social Currents*, *11*(4), 327–345. https://doi.org/10.1177/23294965241228874

Hermawan, A. (2024). Mengintip Celah antara Potensi dan Tantangan Big Data pada Layanan Jaminan Sosial Ketenagakerjaan Indonesia. *Jurnal Jamsostek*, *2*(2), 185–206. https://doi.org/10.61626/jamsostek.v2i2.59

McConville, M. (2017). *Research Methods for Law*. Edinburgh University Press.

Nasution, M. F. (2023). The Role of Civil Law in the Protection of Privacy and Personal Data. *Innovative: Journal Of Social Science Research*, *3*(2), 3669–3679.

Roemmich, K., Rosenberg, T., Fan, S., & Andalibi, N. (2023). Values in Emotion Artificial Intelligence Hiring Services: Technosolutions to Organizational Problems. *Proc. ACM Hum.-Comput. Interact.*, *7*(CSCW1), 109:1-109:28. https://doi.org/10.1145/3579543

Ventura, M., & Coeli, C. M. (2018). Beyond privacy: The right to health information, personal data protection, and governance. *Cadernos de Saúde Pública*, *34*, e00106818. https://doi.org/https://doi.org/10.1590/0102-311X00106818

Versaci, G. (2018). Personal Data and Contract Law: Challenges and Concerns about the Economic Exploitation of the Right to Data Protection. *European Review of Contract Law*, *14*(4), 374–392. https://doi.org/10.1515/ercl-2018-1022

Wu, A.-C., & Kao, D.-D. (2022). Mapping the Sustainable Human-Resource Challenges in Southeast Asia's FinTech Sector. *Journal of Risk and Financial Management*, *15*(7). https://doi.org/10.3390/jrfm15070307

Xiaying, M. (2019). The Legal Attributes of Electronic Data and the Positioning of Data in Civil Law*. *Social Sciences in China*, *40*(1), 82–99. https://doi.org/10.1080/02529203.2018.1519208

Yu, X., & Zhao, Y. (2019). Dualism in data protection: Balancing the right to personal data and the data property right. *Computer Law & Security Review*, *35*(5), 105318. https://doi.org/10.1016/j.clsr.2019.04.001

Yudha, Sahril, I., & Atmadja3, D. A. R. W. (2025). Perlindungan Data Pribadi Konsumen, Dokumen dan Tanda Tangan Elektronik yang Dipergunakan oleh Pihak Ketiga dalam Transaksi E-Commerce. *CENDEKIA : Jurnal Penelitian Dan Pengkajian Ilmiah*, *2*(2), 173–189. https://doi.org/10.62335/cendekia.v2i2.897

Pemerintah Republik Indonesia. (2022). *Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi*. Lembaran Negara Republik Indonesia Tahun 2022 Nomor 197. Sekretariat Negara.