Digital Transformation in Manufacturing and Legal Aspects of Data Protection and Workers

Ricard Osean, Dharma Setiawan Negara, Arif Rachman Putra

Universitas Sunan Giri Surabaya, Indonesia

ARTICLE INFO

Article history:
Received 19 November 2023
Revised 5 December 2023
Accepted 18 December 2023

Key words:
Digital transformation,
Manufacturing,
Personal data protection,
Employee rights,
Business law,
Employment,
Electronic systems.

ABSTRACT

Digital transformation in the manufacturing sector is changing the way companies manage production processes, supply chains, and human resources, with a high dependence on data processing and electronic systems. This study aims to analyses the implications of implementing digital transformation on data protection and workers' rights in manufacturing companies from a normative legal business perspective. The primary legal materials include Law Number 11 of 2020 concerning Job Creation and Government Regulation Number 5 of 2021 concerning risk-based business licensing, Law Number 3 of 2014 concerning Industry, Law Number 27 of 2022 concerning Personal Data Protection, Law Number 11 of 2008 in conjunction with Law Number 19 of 2016 concerning Electronic Information and Transactions, Law Number 13 of 2003 concerning Manpower along with the latest amendments, Law Number 21 of 2000 concerning Labor Unions, as well as regulations concerning occupational safety and health. Qualitative analysis was conducted by interpreting norms, mapping the interrelationships between instruments, and assessing their suitability for digital transformation practices in the manufacturing environment. The results of the study show that digital transformation requires companies to reorganize their licensing governance, electronic system security, management of workers' personal data, and employment patterns that are increasingly dependent on data-based monitoring. The legality of business activities through OSS, compliance with personal data protection principles, respect for the right to organize, and the implementation of OSH in the digital production environment are the main foundations to ensure that technological innovation does not result in violations of workers' rights. This study concludes that the existing legal framework is essentially adequate, but its successful implementation depends on management's commitment to developing internal policies that are in line with regulations and involving workers in decision-making processes related to digitalization.

INTRODUCTION

Digital transformation in the manufacturing industry has changed the way companies design production processes, manage supply chains, and conduct comprehensive quality control. The application of technologies such as the Internet of Things (IoT), big data analytics, cloud computing, and advanced automation has encouraged companies to shift from conventional operating models to highly connected, data-driven systems. These changes have resulted in cost efficiencies, increased productivity, and accelerated product innovation, but at the same time have given rise to new governance over information flows, working relationships, and organizational structures. This new governance must seriously consider the vulnerabilities inherent in the digital ecosystem. As Gardi and Eddine (2023) remind us, cybersecurity and personal data protection in the digital age have become urgent global challenges, requiring collaboration and comprehensive strategies. In theory, digitalization is often understood as a continuation of the industrial revolution that blurs the boundaries between physical and digital entities through cyber-physical systems, so that business decision-making is increasingly influenced by algorithms, digital platforms, and global data infrastructure (Schwab, 2016).

In this technology-laden business environment, manufacturing companies face a heavy dependence on the collection, processing, and storage of data,

** Corresponding author, email address:* ***dr.dharmasetiawannegara@gmail.com***

both operational data and the personal data of workers and business partners. The use of cloud-based enterprise resource planning (ERP) systems, biometric attendance systems, sensor-assisted productivity monitoring, and human resource information system (HRIS) applications has resulted in the expansion of corporate surveillance of workers' bodies and behavior. Similar challenges in balancing digital innovation with the protection of individual rights also occur in other sectors. For example, Aziz et al. (2023) examined the effectiveness of personal data protection regulations in the fintech sector in Indonesia. This digital transformation not only changes production processes but also reproduces inequalities in the labor market. Arifin and Darmawan (2021) emphasize that the gap in access to technology and digital skills between the world of education and the world of work widens the opportunity gap, which can further weaken workers' position in the face of data extraction and surveillance in the workplace. Zuboff (2019) shows that the logic of surveillance capitalism encourages business entities to extract human behavioral data as a new source of economic value, thereby placing serious pressure on the protection of workers' human rights, dignity and privacy.

Not only in social media spaces, digitized workspaces have also become a new arena for norm formation. Costa et al. (2022) examined how interactions on social media shape individuals' self-identity and social perceptions. Similar logic of interaction and surveillance is now spreading to the workplace. In Indonesia, this change is occurring in tandem with the acceleration of Industry 4.0 policies, so that digital transformation in manufacturing is developing within a regulatory framework that is still in progress, including regulations related to personal data protection, electronic system security, and employment (Sinaga & Putri, 2020). More than just a matter of regulation and economics, the intense use of surveillance technology is also changing the cultural landscape and social practices in the workplace. Al Hakim et al. (2021) explain that the digital era has brought about a profound transformation in cultural values and patterns of social interaction, which in the workplace can manifest as the normalization of surveillance, changing expectations of privacy, and a redefinition of the boundaries between work and personal life. This fundamental change in workplace social dynamics is consistent with the findings of Darmawan et al. (2023), who explored the transformation of the relationship between management and employees in multinational companies in the era of literacy-based digitalization, where the digital literacy gap can exacerbate power imbalances. Thus, pressure on workers' human rights and dignity stems not only from data extraction for economic value, but also from changes in social norms that distort power relations in the workplace.

In line with the national legal architecture, manufacturing companies cannot simply view digital transformation as a management technology issue, but rather as a process that requires a restructuring of legal relations between business actors, the state, and workers (Jamaludin et al., 2022). These new legal relations are manifested, among other things, in digital contractual instruments. As analyzed by Rianto et al. (2023) and Sulaiman et al. (2023), the validity and effectiveness of electronic contracts are key pillars in the legal protection of digital transactions in Indonesia. Regulations on electronic information and transactions, data confidentiality, employment relationships, occupational safety and health, and labor supervision create multiple obligations for industry players. On the one hand, the state encourages the adoption of technology to increase manufacturing competitiveness. On the other hand, legal instruments require the application of the principle of prudence regarding data security and the protection of workers' rights. The tension between the drive for efficiency through automation and the necessity to respect the normative rights of workers is what places business law in a strategic position as a balancing framework.

A hermeneutic approach to this development shows that digital transformation is not merely a technical shift, but also a change in the way we interpret work, supervision, and corporate responsibility towards the human subjects behind the numbers and algorithms. Workers in the manufacturing industry are increasingly being reduced to a set of performance indicators that are continuously recorded in digital systems, challenging their autonomy and agency. In response to this reality, government policies to improve human resource competencies based on digital technology, as analyzed by Rojak (2024), are relevant not only for pursuing efficiency but also for empowering workers to understand, manage, and critique the digital systems that govern their work. While Baraja et al. (2023) discuss the implementation and enforcement of data protection laws on online platforms involving business-to-consumer relationships, labor relations in the digital manufacturing ecosystem create more complex implementations due to the involvement of

hierarchies and economic dependencies. On the other hand, management is required to formulate internal policies that are in line with the principles of labor law, personal data protection principles, and information security standards. Within the framework of business law, this transformation needs to be examined normatively to assess the extent to which positive regulations in Indonesia are able to respond to this new reality and provide legal certainty for companies as well as adequate protection for workers (Schwab, 2016; Zuboff, 2019).

The first issue concerns the certainty and coherence of legal regulations that bind manufacturing companies when digitizing business processes. The implementation of data-based production systems requires compliance with various legal instruments, ranging from regulations on data protection and electronic system security to labor regulations concerning employment relationships, wages, and supervision. Challenges arise when companies must interpret their legal obligations in a regulatory environment that is scattered across various laws and implementing regulations, while business practices are evolving rapidly. The literature on the fourth industrial revolution emphasizes that the legal framework often lags behind the dynamics of technological innovation, leaving business actors facing grey areas in the application of legal obligations (Schwab, 2016).

The second issue relates to data protection and workers' privacy rights in an increasingly digitalized manufacturing ecosystem. The recording, processing, and storage of highly detailed worker data, ranging from biometric data to daily work patterns, enables companies to compile economically valuable behavioral profiles. Zuboff (2019) points out that aggressive data collection practices have the potential to reduce human subjects to objects of commercial calculation, which can at any time threaten individual freedom and dignity. In industrial relations in Indonesia, an important question is the extent to which the existing legal system can guarantee that digital monitoring mechanisms for workers do not turn into excessive, discriminatory, or discriminatory surveillance practices that violate normative rights protected by law.

The third issue touches on the dimensions of fairness and sustainability of employment relations amid the penetration of automation and artificial intelligence in production lines. Digital transformation opens up opportunities for workforce rationalization, changes in job structures, and the relocation of certain functions from humans to machines or algorithmic systems. Without an adequate legal basis, this process can lead to uncertainty in employment status, reduction of rights, and marginalization of certain groups of workers who find it difficult to adapt. From a business law perspective, the question that arises is how the principles of fairness, propriety, and good faith inherent in business operations are applied when companies redesign their organizations and employment relationships based on advanced technology (Schwab, 2016; Zuboff, 2019). A normative legal review is needed to map the potential conflict between corporate efficiency interests and the obligation to protect workers.

Studies on the legal aspects of digital transformation in manufacturing companies are highly relevant in the acceleration phase of Industry 4.0 in Indonesia, where the government is promoting the digitization of production processes through various policy initiatives. This push is not only about efficiency, but also about creating a fair digital economy. In line with this, Sudiruddin et al. (2023) emphasize the importance of optimizing the principles of fair business competition and realizing economic justice in the digital era. Companies striving to survive in global competition are driven to rapidly adopt automation, robotics, and integrated information systems. In such a situation, the application of legally compliant business governance principles risks being neglected if companies place technological innovation as their sole priority. Analysis based on normative legal methods allows for mapping existing legal obligations and identifying areas that require regulatory updates to ensure that digitalization does not erode protection for the most vulnerable subjects, namely manufacturing workers at the operational level.

Furthermore, at the global level, there is a broad discourse on digital capitalism and massive data collection practices by corporations, which raises new issues related to human rights, data sovereignty, and corporate accountability (Zuboff, 2019). Indonesia, as a country with a large manufacturing base and workforce, is not immune to this trend. The absence of adequate business law studies has the potential to expose companies to significant legal risks in the future, whether in the form of industrial relations disputes, administrative sanctions, or civil lawsuits related to data and worker rights violations. Research that explicitly links the digital transformation of manufacturing with compliance obligations regarding regulations, data security, and the protection of workers' rights can provide a conceptual basis for the formulation of corporate policies and recommendations for more responsive regulatory updates.

This study aims to conduct a normative legal analysis of the legal compliance obligations of manufacturing companies in the digital transformation process, with an emphasis on the interrelationship between applicable regulations on data security, electronic systems, and the protection of workers' rights in Indonesia. Theoretically, this study seeks to enrich the study of business law regarding the digitalization of the manufacturing industry by showing how the principles of labor law and personal data protection bind managerial practices in the era of Industry 4.0. In practical terms, this study is expected to provide a reference for company management, policy makers, and industrial relations stakeholders in designing internal policies and regulations that are consistent with the national legal framework while being adaptive to technological developments.

RESEARCH METHOD

The research method used in this study is a normative juridical method with a qualitative literature study approach. The main focus is on analyzing legislation, legal doctrines, and court decisions relevant to digital transformation in manufacturing companies, including aspects of regulatory compliance, data security, and workers' rights. Normative legal research was chosen because the issues examined relate to how positive law regulates and should guide the practice of digital transformation in a corporate environment. The main data used were primary legal materials (laws, government regulations, OJK regulations, Ministry of Manpower regulations, data protection regulations, etc.) and secondary legal materials (books, journal articles, official reports). The analysis was conducted qualitatively by interpreting norms, tracing the relationships between provisions, and identifying normative tensions that arise when digital technology is widely adopted in manufacturing business processes.

The literature search strategy was carried out systematically through legal and business journal databases, academic publisher catalogues, and official government agency portals. The keywords used included "normative legal research", "business law and digital transformation", "data security and manufacturing companies", "workers' rights and industrial automation", and similar terms in Indonesian and English. Inclusion criteria were set based on several parameters: (1) published within the last twenty years; (2) discussing the legal aspects of digitalization, the manufacturing industry, employment, or data protection; (3) academic or official in nature (journals, scientific books, policy reports). Exclusion criteria were applied to popular writings, news articles, or corporate promotional material. Primary legal materials were selected by tracing the hierarchy of regulations applicable in Indonesia, from laws to administrative regulations, to ensure that all regulations relevant to digital transformation in the manufacturing sector were covered.

The analysis process was carried out through thematic synthesis of the collected legal materials and literature. The initial stage involved open coding to identify key themes, such as corporate compliance obligations with digital regulations, data security and protection standards, changes in employment relationships due to automation, and mechanisms for protecting workers' rights in the digital workplace. The next stage was axial coding to link these themes to general principles of business law, labor law, and data protection law. The quality of the analysis is ensured through triangulation between sources (comparing regulations, doctrines, and court decisions), checking the consistency of the interpretation of norms, and limiting claims to remain in line with the available normative data. In this way, the research is expected to produce a systematic mapping and academically accountable arguments regarding the legal aspects of digital transformation in manufacturing companies.

RESULT AND DISCUSSION

Legal Compliance Framework in the Digital Transformation of Manufacturing Companies

The nature of digital transformation in manufacturing companies essentially changes almost the entire value chain, from production planning, raw material procurement, automation and sensor-based manufacturing processes, to product distribution with real-time monitoring systems. These processes are highly dependent on large-scale data processing, network connectivity, and system integration with various business partners. From a business law perspective, these conditions require a clear framework for compliance with laws and regulations governing electronic information and transactions, data protection, electronic system security standards, and the protection of workers involved in the digital production process chain. In Indonesia, this framework has been developed gradually, starting with general regulations on electronic information and transactions, regulations on electronic system operators and data centers, to sectoral policies on

industry and employment. For manufacturing companies, the main challenge lies in how to develop internal governance so that all digital processes carried out do not conflict with the provisions set by the state, while maintaining efficiency and competitive advantage.

The basic regulations on the use of information technology in business activities in Indonesia are rooted in Law No. 11 of 2008 on Electronic Information and Transactions, as amended by Law No. 19 of 2016 (Hidayah, 2019). For manufacturing companies, the provisions in this law frame the validity of electronic documents, electronic transaction mechanisms, the obligation to maintain the integrity and availability of information, and the responsibilities of electronic system operators. When production, procurement, and distribution systems are integrated into a digital platform, all order data, contracts, and transaction records stored electronically fall under the scope of this law (Jamaludin et al., 2022). This means that companies must ensure that the systems they use are capable of guaranteeing the authentication, integrity, and confidentiality of information in accordance with the minimum standards set by the regulations. If a disruption, leak, or manipulation of data affects business contracts or product quality, the legal liability framework used will refer, among other things, to the ITE regime and its derivative regulations (Hendrawan, 2022; Susanti, 2022).

Further implementation of the obligations of electronic system operators is regulated in various government regulations and ministerial regulations that are binding on business actors. One important reference is the provisions regarding the operation of electronic systems and transactions, which require the implementation of auditable security standards, risk management, and information technology governance. Although initially adopted for the financial services and public services sectors, these standards are slowly spreading to the manufacturing sector, which is increasingly dependent on digital platforms to manage supply chains and customer relationships. This dependence is increasing in line with efforts to optimize supply chains through digital transformation. One such optimization effort is the management of big data for strategic decision-making, as studied by Ali and Darmawan (2023). However, according to Putra and Arifin (2021), the adoption of big data, artificial intelligence, and the Internet of Things (IoT) in manufacturing supply chain management is a key trend that actually increases exposure to cyber risks, thereby emphasizing the urgency of complying with technology security and governance standards. Manufacturing companies that operate their own data centers, or utilize third-party data centers, must pay attention to provisions regarding data center placement, disaster recovery capabilities, and incident reporting procedures to the authorities. Neglecting these obligations can have legal consequences, ranging from administrative sanctions to potential civil lawsuits if business partners or consumers suffer losses.

The dimension that is currently strengthening in the compliance framework is personal data protection, including employee data and business partner data processed in digital-based manufacturing systems. On the one hand, employee data collected from digital systems is a strategic asset. As shown by Khairi and Darmawan (2022), developing data analysis capabilities in HR functions can encourage more effective decision-making within organizations. However, on the other hand, the dimension that is currently strengthening in the compliance framework is the protection of personal data itself, including employee data and business partner data processed in digital-based manufacturing systems. In the factory environment, the use of Internet of Things devices, biometric sensors, digital attendance systems, data-based performance monitoring, and integration with human resource applications generates a large and constantly updated collection of personal data (Sinaga & Putri, 2020). At the regulatory level, Indonesia has adopted its own regulations on personal data protection, which govern the principles of lawful processing, clear purposes, storage limits, data subject rights, and the obligations of data controllers and processors. Manufacturing companies undergoing digital transformation must read these regulations in conjunction with labor and ITE regulations, as workers' personal data is processed within the framework of employment relationships, which have their own consequences. Failure to comply with data protection principles, such as excessive data collection without a legitimate basis or disclosure to third parties without consent, has the potential to give rise to claims of privacy violations.

In addition, the labor law framework remains the main reference when digital transformation brings changes to work patterns, supervision, and the competency structure of workers in the manufacturing sector. Law No. 13 of 2003 concerning Manpower, as amended by Law No. 11 of 2020 concerning Job Creation and its implementing regulations, regulates the principles of worker protection, employment relationships, termination of

employment, and decent working conditions. When companies adopt automation, artificial intelligence, and robotics to replace or reinforce the role of workers, consideration must be given to how changes in job structures, shifts in competencies, and possible workforce reductions can be accommodated within this framework of protection. Digital transformation cannot be used as a reason to disregard workers' basic rights regarding wages, social security, working hours and rest periods, and the right to a safe working environment. This requires adjustments to employment agreements, company regulations, and collective bargaining agreements to align with the new practices brought about by digitalization.

The regulatory framework regarding occupational safety and health has gained new relevance as manufacturing companies implement digital production systems and automation. The Occupational Safety and Health Act, along with its implementing regulations, requires employers to ensure safe and healthy working conditions, including when workers interact with automated machines, industrial robots, or smart devices. Workplace accidents in a digitalized production environment can arise not only from mechanical factors, but also from software system failures, incorrect sensor integration, or data manipulation that causes system commands to run improperly. In this context, compliance with technical safety standards must be integrated with good electronic system management procedures, such as periodic testing, access authorization, and documentation of changes to production software. Regulations require employers to conduct training, provide personal protective equipment, and establish accident reporting systems, all of which need to be aligned with information technology governance in digital factories.

Digital transformation in the manufacturing sector also intersects with consumer protection law when products are manufactured and marketed through digital channels (Jamaludin et al., 2022). Consumer protection laws and their derivative regulations require that information about products, quality, and after-sales guarantees be conveyed accurately and not misleadingly, including when distributed through e-commerce platforms, company online portals, or data-based after-sales service applications. The use of customer data for product maintenance, remote monitoring, or service personalization must take into account the limitations of personal data protection (Sinaga & Putri, 2020). At the same time, if a manufacturing defect occurs that is related to a digital system failure (e.g., an algorithm error in machine settings), product liability may extend to the system owner or technology provider. This emphasizes that manufacturing companies undergoing digitalization are not merely making technical changes, but also expanding the scope of legal risks that must be anticipated through compliance programmers.

From a corporate legal and governance perspective, compliance obligations with digital and labor regulations are closely related to the responsibilities of corporate bodies, particularly the board of directors and board of commissioners. The Limited Liability Company Law requires directors to manage the company in good faith and with full responsibility. In the era of digital transformation, this standard of care requires directors to proactively identify the legal implications of adopting new technologies, ensuring that internal control systems are adequate to address the risks of data leaks, system failures, or worker rights violations. The board of commissioners is obliged to supervise the digitalization policies adopted by management, including technology outsourcing policies, data sharing agreements with partners, and employee retraining programmers. If failure to comply with digital and labor regulations causes significant material or reputational damage to the company, the potential liability of directors and commissioners may be examined based on applicable fiduciary duty standards.

Furthermore, failure to manage these digital risks can quickly turn into a widespread reputation crisis in the online space. Darmawan et al. (2022) emphasize that maintaining a positive image on social media and in the digital environment is a complex challenge for corporations, where a single incident of data security or worker rights violations that goes viral can result in significant and long-lasting damage to reputation. Thus, the duty of care and loyalty of corporate bodies in digital transformation also includes the proactive responsibility to protect the company's reputation assets.

In practice, manufacturing companies in Indonesia often find themselves in a middle ground: on the one hand, they are driven to pursue Industry 4.0 agendas and improve efficiency through automation and system integration; on the other hand, they must navigate a regulatory landscape that is scattered across various sectors. Government policies on the industry 4.0 roadmap provide strategic direction, but are not always explicitly integrated with regulations on data protection, employment, and occupational safety. Companies then need to develop

an internal compliance map that maps each digital initiative such as installing sensors on production lines, implementing workforce management applications, or integrating with logistics platforms to relevant regulations. This task is not merely administrative, but rather serves as a basis for assessing whether the adopted technology design is in line with applicable legal principles, such as the principles of prudence, proportionality, and respect for human dignity in employment relationships.

Another important aspect is coordination between government agencies that oversee areas related to digital transformation in the manufacturing sector. Authorities that regulate industry, employment, data protection, and telecommunications and information technology have different mandates, but their objectives often overlap. For businesses, this fragmentation of authority can create uncertainty about which standards to follow when designing and operating digital systems. For example, the information security standards required by one ministry may differ in detail from the guidelines of another agency. Therefore, companies need to adopt internal standards that refer to international best practices without neglecting mandatory national provisions. At this point, the role of internal and external legal advisors is crucial, as they must be able to translate cross-sector regulatory developments into operational guidelines that can be understood by engineers, production managers, and software developers.

In terms of labor relations, digital transformation often creates tension between the need for production efficiency and the protection of workers' dignity. The use of real-time performance monitoring systems, for example, can increase productivity and reduce machine downtime, but at the same time raise concerns among workers about excessive surveillance and the possible use of data for disproportionate disciplinary purposes. Indonesian labor law provides a basis for workers to demand clarity regarding performance appraisal procedures, objection mechanisms, and protection from discriminatory actions. Therefore, when companies change from manual form-based assessment systems to digital systems that automatically collect work behavior data, these changes should be accompanied by consultation with worker representatives and adjustments to company regulations. In this way, workers' rights to information, participation, and protection from arbitrary treatment are maintained amid the tide of digitalization.

Companies need to build an integrated compliance framework that links information technology regulations, data protection, employment, occupational safety, and consumer protection into clear operational guidelines. This requires an inventory of the digital systems used, mapping of data flows, identification of risk points, and designation of responsible parties at the management level. Commitment to security and compliance principles from the initial design stage can be manifested through the selection of appropriate technology. For example, a study by Costa et al. (2023) proposes the use of blockchain technology in HR systems to secure employee data, which is essentially the application of secure design principles and transparent and immutable access governance to meet data protection obligations. This approach will help companies avoid reactive compliance, which is only implemented after an incident or authority inspection. Instead, compliance can be part of the initial design of every digitization project, so that the choice of technology architecture, access governance, and human resource policies are tailored from the outset to the limits outlined by law.

Digital transformation should be viewed as an ongoing legal and managerial process, not a short-term technology project. The national regulatory landscape will continue to evolve in line with technological developments and public demands for data protection and workers' rights. Manufacturing companies that want to survive and grow need to establish regulatory monitoring mechanisms, regularly update internal policies, and implement transparent communication programmers for workers and business partners regarding how data is used and what rights they can claim. By making legal compliance an integral part of their digital strategy, companies not only reduce the risk of sanctions and disputes, but also build trust, which ultimately becomes an important asset in an increasingly networked and data-driven industry.

The Implications of Digital Transformation on Data Protection and Workers' Rights within the Business Law Framework

The implementation of digital transformation in manufacturing companies has brought about major changes in the way companies process employee data, manage labor relations, and carry out daily operations (Jamaludin et al., 2022). On the one hand, technologies such as IoT and big data increase efficiency, but on the other hand, dependence on data has expanded surveillance of workers and has the potential to deepen inequalities due to the digital skills gap (Arifin & Darmawan, 2021). This transformation also strengthens the legal compliance dimension,

especially in the protection of personal data, which is now regulated by the PDP Law. Hermeneutically, these changes are not merely technical but represent a shift in the meaning of work, where workers are often reduced to a set of performance data. Therefore, normative legal studies are needed to assess the adequacy of legal protection for workers in the digital era (Schwab, 2016; Zuboff, 2019).

From a normative legal business perspective, these changes must be viewed in conjunction with the licensing framework, data protection, and labor regulations. Through Law No. 11 of 2020 on Job Creation, the state is promoting ease of doing business by digitizing the licensing process through the Online Single Submission (OSS) system. For manufacturing companies, the use of OSS is not merely an administrative matter, but determines the legality of business activities and the authority to operate digitized production facilities. In addition, Government Regulation Number 5 of 2021 concerning the Implementation of Risk-Based Business Licensing requires companies to assess the level of risk of business activities, which will have an impact on the obligation to meet standards, including technological and electronic system security standards. Thus, digital transformation cannot be separated from the obligation to organize permits and business commitments in accordance with the risk structure set by regulations.

Law No. 3 of 2014 concerning Industry stipulates that industry players must comply with technology and innovation standards, including the application of production processes that lead to high-tech industrialization. The obligation to comply with these technological standards, when read in conjunction with the push for Industry 4.0, encourages manufacturing companies to adopt automation, the Internet of Things, and production data integration. However, the obligation to innovate technologically in the Industry Law does not mean absolute freedom for companies to collect and process employee data without limits. The technological transformation desired by the law must be balanced with respect for workers' rights as regulated in labor laws and personal data protection regulations. From a business law perspective, management is obliged to formulate internal policies that ensure that investments in new technology do not violate other regulations that bind companies as private legal entities and industrial players supervised by the state.

Data protection has gained a strong legal foundation through Law No. 27 of 2022 on Personal Data Protection (PDP Law). A study by Issalillah and Hardyansah (2022) shows that digital transformation can widen the participation gap and erode trust at the community level due to the digital divide and misinformation. At a more micro and regulatory level, this social framework is reinforced by the analysis of Zulkarnain and Al Hakim (2023), which reveals how the evolution of digital media shape's public opinion with serious implications for the credibility of information and social dynamics. Amidst these socio-digital dynamics, the dimension of data protection at a more micro and regulatory level has gained a strong legal foundation through Law No. 27 of 2022 concerning Personal Data Protection (PDP Law). For manufacturing companies that are digitizing their human resources, supply chain, and IoT-based production operations, almost every step of workforce management will generate and rely on workers' personal data. The PDP Law stipulates that the collection, storage, and processing of personal data must be based on legitimate grounds for processing, including consent, the fulfilment of legal obligations, the execution of agreements, or certain legitimate interests that are balanced with the rights of data subjects. This implies that companies should not use digital transformation as an excuse to store biometric data, performance history, and employee behavior patterns excessively beyond what is reasonably necessary. The obligations of information transparency, purpose limitation, technical security, and respect for the rights of access, correction, and deletion of employee data place companies in a position of accountability for the entire life cycle of data generated by digital systems in the workplace.

Law No. 11 of 2008 concerning Electronic Information and Transactions, as amended by Law No. 19 of 2016 (ITE Law), complements the PDP Law by regulating the obligations of electronic system operators and their responsibility for system security breaches (Sinaga & Putri, 2020). In manufacturing companies, digital attendance systems, payroll portals, HR applications, and sensor-based production systems are considered "electronic systems" according to the definition of the ITE Law. These regulations require the implementation of adequate security governance, maintaining the integrity, availability, and confidentiality of information, as well as providing recovery mechanisms in the event of a disruption. For workers, an employer's failure to maintain the security of electronic systems can result in the misuse of personal data and other losses, such as delayed wages due to cyber-attacks or manipulation of performance data resulting in unfair disciplinary

sanctions. From a business law perspective, negligent companies may face civil and administrative liability, so the design of information technology architecture must be aligned with the principle of prudence reflected in the ITE Law.

The link between digital transformation and financial and payment systems is also becoming increasingly clear as manufacturing companies integrate Enterprise Resource Planning (ERP), digital payroll modules, or application-based payment schemes connected to banking and fintech systems. In this case, Bank Indonesia and Financial Services Authority regulations regarding payment system security, financial services consumer protection, and information technology risk management become relevant even though manufacturing companies are not financial institutions. If manufacturers use payment gateway services, electronic wallets, or real-time integration with banks to pay workers' wages and incentives, then the security and data protection standards required by financial services regulators indirectly become a benchmark for companies' prudence. Neglecting these standards has the potential to give rise to disputes over responsibility between payment service providers, manufacturing companies, and workers in the event of data leaks or wage transaction failures.

In the realm of labor relations, Law No. 13 of 2003 on Manpower, several provisions of which were amended by Law No. 11 of 2020 on Job Creation and later confirmed by Law No. 6 of 2023, remains the primary reference for assessing whether digital transformation respects workers' basic rights. Digital labor relations do not eliminate the employer's obligation to provide decent wages, social security, work and rest time arrangements, and protection against termination of employment. For example, when a company implements an algorithm-based automatic work scheduling system, the arrangement must still comply with the maximum working hours and leave entitlements as stipulated in the Manpower Law. If performance data collected through production line sensors is used as the basis for mass layoffs without dialogue and without reasonable justification, such actions could potentially conflict with the principle of worker protection under the labor regime and pose the risk of industrial disputes.

Law No. 21 of 2000 concerning Trade Unions/Labor Unions grants workers the right to form and join unions that legally represent their interests in the workplace (Podungge et al., 2021). In the digital age, this right includes the space to negotiate the application of new technologies that impact workload, surveillance, and personal data security. Labor unions have the right to obtain information from employers regarding automation plans, the implementation of digital monitoring systems, and policies on the use of performance data for disciplinary or promotional purposes (Jamaludin et al., 2022). If a company implements HR applications without adequate consultation and uses data unilaterally, thereby weakening the bargaining position of workers, the union can raise objections through bipartite or tripartite negotiation mechanisms in accordance with the applicable legal framework. From a business law perspective, involving trade unions from the outset helps reduce the risk of conflict and provides social legitimacy to the digital transformation programmed designed by management.

Digital transformation arrangements also intersect with occupational safety and health aspects, which are the main mandate of OSH regulations and the ministerial regulations governing them. The implementation of industrial robots, remote control systems, and the use of wearable devices in factories presents new risk patterns. OSH regulations require employers to identify hazards, assess risks, and control risks, including those arising from software system failures or human-machine interfaces. Sensor-based worker condition monitoring systems, for example, can help prevent accidents, but at the same time generate highly sensitive health data. The legal implications are that companies must balance their obligation to protect workplace safety with their obligation to keep workers' health data confidential under the Personal Data Protection Act and to maintain workers' dignity in accordance with general labor principles. Violations of OSH standards in a digital environment can result in administrative and criminal sanctions and claims for damages.

The Job Creation Law and Government Regulation No. 5 of 2021, with an emphasis on risk-based licensing, have direct implications for managerial responsibility in mapping the legal risks of digital transformation. If digital production activities are classified as medium-high or high risk, companies are required to meet certain standards, including possible certification requirements, periodic reporting, or technical audits. For data protection and workers' rights, this risk classification can be interpreted as a normative basis that reinforces the requirement for stricter information security management and employment management. Within the business legal framework, neglecting risk-based licensing obligations is not merely an administrative violation, but can also be used as an indicator of managerial negligence in the

event of a data breach or work accident related to digital systems. In other words, licensing regulations serve as a foundation that links technical compliance and the protection of human rights in the workplace.

Law No. 6 of 2023, which stipulates the Job Creation Perppu into law, confirms the adjustment of labor regulations to the reality of a technology-based economy, among others by providing flexibility in the regulation of certain types of employment agreements, outsourcing, and working hours. For manufacturing companies that adopt flexible work models based on digital systems, such as dynamic scheduling, partial remote working for certain functions, or system-recorded achievement-based incentives, this flexibility can facilitate workforce management. However, legally, flexibility must not eliminate the basic principles of worker protection. The right to social security, freedom of association, and protection from arbitrary termination of employment must still be upheld. If internal regulations rely on non-transparent assessment algorithms that make it difficult for workers to defend themselves, then the structure of digital employment relationships has the potential to conflict with the spirit of the Manpower Act and the Trade Union Act, thereby weakening the social legitimacy of the company in the eyes of workers and other stakeholders (Podungge et al., 2021).

From a business law perspective, these regulations form a normative field that companies must negotiate through planned governance. The practical implication for manufacturing company management is the need to establish an integrated compliance framework that combines risk-based OSS licensing, personal data protection obligations, electronic system security standards, labor regulations, union rights, and occupational health and safety regulations. This framework is then translated into policies on the use of employee data, approval and notification procedures, access and authorization matrices in digital systems, and accountable performance appraisal and work discipline procedures. A clear distinction between data that is necessary for safety and efficiency, and data that is excessive and invasive, is key to ensuring that digital transformation does not lead to violations of workers' human rights in factories.

The normative implications outlined above can be summarized as the basis for developing a managerial strategy oriented towards compliance and respect for workers' dignity. First, manufacturing companies need to view every digitalization project from production line automation to the implementation of HR platforms as a legal action that creates new obligations, not merely technical innovations. Every initiative should be preceded by a legal compliance review that examines the relevance of the technology plan to the Job Creation Law, Government Regulation No. 5/2021, the Industry Law, the ITE Law, the PDP Law, the Manpower Law, the Trade Union Law, and K3 regulations. This review encourages management to choose technology solutions that are more worker-friendly, reduce excessive monitoring, and ensure that data used for performance appraisals can be audited.

Second, from a normative legal perspective, digital transformation should ideally strengthen, not weaken, the position of workers as protected legal subjects. Companies can use data protection and labor regulations as guidelines for developing transparent internal procedures, for example by giving workers access to their performance data, establishing mechanisms for appealing algorithm-based decisions, and ensuring that labor unions are involved in the development of digital policies. Such an approach helps reduce the potential for disputes and increases trust, which ultimately benefits companies in terms of business continuity. Thus, digital transformation in Indonesia's manufacturing sector can proceed within a clear legal framework, maintaining a balance between corporate efficiency and respect for workers' rights and personal data protection.

CONCLUSION

Digital transformation in manufacturing companies is changing the way data is managed and the way working relationships are conducted. From a normative legal study, it appears that the business legal framework in Indonesia still provides ample room for innovation, but at the same time places strict obligations on business actors to maintain the legality of permits, protect personal data, and respect workers' rights. Regulations concerning risk-based business licensing, the obligation to comply with industry technology standards, personal data protection, electronic systems, employment, freedom of association, and occupational health and safety are normatively intertwined. When formulated consistently, this set of regulations can serve as a legal safeguard to ensure that digital transformation in the manufacturing sector is carried out legally, safely, and with respect for the dignity of workers as protected legal subjects.

This study shows that manufacturing companies that are undergoing or will undergo digital transformation need to reorganize their business governance by making regulatory compliance part of the initial design, rather than just an administrative

obligation later on. Management is required to develop internal policies that combine risk-based OSS licensing obligations, personal data protection in accordance with the PDP Law and ITE Law, protection of workers' rights in accordance with the Manpower Law, Trade Union Law, and K3 obligations. The practical implications are the need for an internal regulatory map, a mechanism for assessing the legal risks of each digital project, and procedures that enable workers to understand and monitor the use of their data. Thus, digital transformation can become a source of business excellence that is in line with positive legal provisions.

Manufacturing companies are advised to form cross-functional teams involving legal, information technology, human resources, and OSH elements to assess each digital initiative before implementation. The government and supervisory agencies are expected to strengthen cross-sector regulatory harmonization, particularly between industry, labor, data protection, and payment systems, while providing applicable guidelines for manufacturing businesses. Workers and labor unions need to improve their digital legal literacy in order to participate constructively in negotiations on monitoring policies, data use, and changes in work patterns due to automation. Further research is recommended to explore concrete practices at the company level to assess the extent to which the existing regulatory framework has been implemented and what obstacles have arisen in the field.

REFERENCES

Al Hakim, Y. R., Rojak, J. A., & Triono, B. (2021). Transformation of Cultural Values and Social Practices in the Digital Age. *Journal of Social Science Studies*, 1(1), 173-178.

Ali, R., & Darmawan, D. (2023). Big Data Management Optimization for Managerial Decision Making and Business Strategy. *Journal of Social Science Studies*, 3(2), 139-144.

Arifin, S., & Darmawan, D. (2021). Technology Access and Digital Skills: Bridging the Gaps in Education and Employment Opportunities in the Age of Technology 4.0. *Journal of Social Science Studies*, 1(1), 163-168.

Aziz, A., Darmawan, D., Khayru, R. K., Wibowo, A. S., & Mujito. (2023). Effectiveness of Personal Data Protection Regulation in Indonesia's Fintech Sector. *Journal of Social Science Studies*, 3(1), 23-28.

Baraja, M. U., Saputra, R., Saktiawan, P., Dirgantara, F., & Waskito, S. (2023). Implementation and Supervision of Personal Data Protection Law on Online Platforms. *Journal of Social Science Studies*, 3(1), 101-108.

costa, S. da, Darmawan, D., & Isaac, A. de J. (2022). Self-Identity Formation and Social Perception of Individuals through Interaction on Social Media in a Digital World. *Journal of Social Science Studies*, 2(2), 273-278.

costa, S. da., Darmawan, D., & Isaac, A. de J. (2023). Safeguarding Employee Data with Blockchain in HR. *International Journal of Service Science, Management, Engineering, and Technology*, 4(3), 41–46.

Darmawan, D., Mendonca, C. N., & Isaac, A. de J. (2022). Managing Corporate Reputation in the Digital Age: Challenges and Solutions for Maintaining a Positive Image on Social Media. *Journal of Social Science Studies,* 2(1), 283-288.

Darmawan, D., Gardi, B., & Da Silva, E. B. (2023). Exploration of Changes in Management and Employee Work Relations in Multinational Companies in the Era of Literacy-Based Digitalization. Journal of Science, Technology and Society (SICO), 4(2), 43-54.

Gardi, B., & Eddine, B. A. S. (2023). Cyber Security and Personal Data Protection in the Digital Age: Challenges, Impacts, and Urgency of Global Collaboration. *Bulletin of Science, Technology and Society,* 2(3), 58–63.

Hendrawan, D. (2022). *The Legality of Trading Through Electronic Systems in Indonesia*. https://doi.org/10.53555/ephhss.v8i1.1901

Hidayah, A. (2019). Konsep Pembangunan Hukum E-Commerce. *Solusi*, 17(2), 106-113.

Issalillah, F., & Hardyansah, R. (2022). The Impact of the Digital Divide and Misinformation on Partici-pation and Trust in Local Communities. *Journal of Social Science Studies*, 2(2), 7-12.

Jamaludin, M., Sulistianto, S. W., A MI, S. P., MM, M., Debby Marthalia, S. P., Rinandita Wikansari, S., ... & Okta Veza, M. (2022). *Transformasi Digital dalam Dunia Bisnis*. Cendikia Mulia Mandiri.

Khairi, M., & Darmawan, D. (2022). Developing HR Capabilities in Data Analysis for More Effective Decision Making in Organizations. *Journal of Social Science Studies,* 2(1), 223-228.

Peraturan Pemerintah Nomor 5 Tahun 2021 tentang Penyelenggaraan Perizinan Berusaha Berbasis Risiko.

Podungge, I. P., Patiolo, D., Silvya, V., & Hanifa, I. (2021). Peran Serikat Pekerja/Buruh dalam Penyelesaian Perselisihan Pemutusan

Hubungan Kerja secara Sepihak yang dilakukan oleh Perusahaan Terhadap Pekerja/Buruh. *Jurnal Hukum Lex Generalis*, 2(5), 384-399.

Putra, A. R., & Arifin, S. (2021). Supply Chain Management Optimization in the Manufacturing Industry through Digital Transformation: The Role of Big Data, Artificial Intelligence, and the Internet of Things. *Journal of Social Science Studies*, 1(2), 161-166.

Rianto, Darmawan, D., & Negara, D. S. (2023). The Application of Restorative Justice in Resolving Speech Cases in the Digital Space: A Normative Analysis of the Electronic Information and Transactions Law and the Criminal Code. *Journal of Social Science Studies*, 3(1), 295-306.

Rojak, J. A. (2024). Government Policy in Improving Human Resource Competencies Based on Digital Technology. *Bulletin of Science, Technology and Society*, 3(2), 1–8.

Schwab, K. (2016). *The Fourth Industrial Revolution*. New York: Crown Business.

Sinaga, E. M. C., & Putri, M. C. (2020). Formulasi Legislasi Perlindungan Data Pribadi dalam Revolusi Industri 4.0. *Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional*, 9(2), 237.

Sudiruddin, Wibowo, A. S., Darmawan, D., Halizah, S. N., & Mardikaningsih, R. (2023). Optimizing the Principles of Healthy Business Competition and the Role of KPPU for a Fair Economy in the Digital Era. *Journal of Social Science Studies*, 3(1), 95-100.

Sulaiman, M., Pakpahan, N. H., & Putra, A. R. (2023). Analysis of the Validity and Effectiveness of Electronic Contracts in Legal Protection of Digital Transactions in Indonesia. *Journal of Social Science Studies*, 3(1), 41-46.

Susanti, D. O. (2022). The electronic market (marketplace) on electronic trade (e-commerce) in indonesia. *NOTARIIL Jurnal Kenotariatan*, 7(1), 24-31.

Undang Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana diubah dengan Undang Undang Nomor 19 Tahun 2016.

Undang Undang Nomor 11 Tahun 2020 tentang Cipta Kerja.

Undang Undang Nomor 13 Tahun 2003 tentang Ketenagakerjaan.

Undang Undang Nomor 21 Tahun 2000 tentang Serikat Pekerja/Serikat Buruh.

Undang Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.

Undang Undang Nomor 3 Tahun 2014 tentang Perindustrian.

Undang Undang Nomor 6 Tahun 2023 tentang Penetapan Perppu Cipta Kerja menjadi Undang Undang.

Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: PublicAffairs.

Zulkarnain, M. A. B., & Al Hakim, Y. R. (2023). Digital Media Evolution and Public Opinion Formation: Implications for Information Credibility and Social Dynamics. *Bulletin of Science, Technology and Society*, 2(1), 49–55.

***R. Osean, D. S. Negara, & A. R. Putra. (2024). Digital Transformation in Manufacturing and Legal Aspects of Data Protection and Workers, *Journal of Social Science Studies*, 4(1), 21– 32.**