

Criminal Liability of Corporations for Worker Supervision Practices Outside Working Hours from the Perspective of Labor Law, Ite Law, and Personal Data Protection

Totok Handono¹, Siti Humulhaer², Muhammad Rizki Azhari³, Harry Sudhana⁴, Dewi Rahayu⁵

Universitas Islam Syekh Yusuf - Tangerang

Article Info

Article history:

Accepted: 24 February 2026

Publish: 1 March 2026

Keywords:

Corporate Criminal Liability;

Employee Surveillance;

Labor Law;

Data Protection.

Abstract

The expansion of digital technology has enabled corporations to conduct employee surveillance beyond working hours through electronic systems and personal data monitoring. Such practices raise legal concerns as they may exceed employer authority under labor law and violate personal data protection principles. This study analyzes the legal limits of off-duty employee surveillance based on Indonesian labor law, electronic information law, and personal data protection law, and formulates corporate criminal liability for such practices. Using normative juridical methods and statutory analysis, the study finds that off-duty surveillance lacks legal basis in labor law, may constitute unlawful electronic access under electronic information law, and represents unlawful personal data processing under data protection law. When implemented as corporate policy, such surveillance fulfills elements of corporate criminal liability. Off-duty employee surveillance constitutes a deviation from statutory limits of corporate authority and infringes workers' privacy rights.

This is an open access article under the [Lisensi Creative Commons Atribusi-BerbagiSerupa 4.0 Internasional](https://creativecommons.org/licenses/by-sa/4.0/)



Corresponding Author:

Totok Handono

Universitas Islam Syekh Yusuf – Tangerang

Email: ttkhandono@gmail.com

1. INTRODUCTION

The employment relationship between a corporation and its employees is a legal relationship arising from an employment agreement and specifically regulated by labor law. Within this relationship, the corporation has the authority to regulate and oversee work implementation as part of its managerial function. However, this authority is not absolute but is limited by legal norms aimed at protecting the dignity, rights, and interests of employees as legal subjects.

Normatively, Law Number 13 of 2003 concerning Manpower affirms that employment relationships are built on the basis of work, wages, and orders. The element of "orders" in the employment relationship provides legitimacy for employers to supervise workers, but such supervision is implicitly limited by workspace and time. Provisions regarding working hours and rest periods as regulated in Articles 77 and 79 of the Manpower Law, indicate that work obligations and controls are attached to specific working hours, so that outside of working hours, workers are in a private space that is no longer under the direct control of the corporation.

In industrial relations (das sein) practices, advances in information technology have encouraged corporations to expand their forms of employee supervision, including

supervision conducted outside of working hours. This supervision can be conducted through various mechanisms, both directly and through the use of electronic systems, which have the potential to generate, collect, and process workers' personal data. Corporations often justify this practice on the grounds of operational interests, work discipline, safety, and company reputation, although the legal boundaries are not always clear.

The use of electronic systems in worker surveillance practices carries legal consequences under the regime of Law Number 11 of 2008 concerning Electronic Information and Transactions as amended by Law Number 19 of 2016. The ITE Law stipulates that any use of electronic systems must be carried out legally and must not violate the rights of others. Provisions regarding the prohibition of unauthorized access and interception of electronic information as stipulated in Articles 30 and 31 of the ITE Law, implicitly emphasize that the use of surveillance technology must not violate the limits of legal authority, including regarding worker data and activities outside of employment relationships.

The legal issue of monitoring workers outside of working hours has become increasingly crucial following the enactment of Law Number 27 of 2022 concerning Personal Data Protection. This law explicitly states that personal data is a human right. Article 1, number 1 of the Personal Data Protection Law defines personal data as any data about an identified or identifiable natural person. Furthermore, Articles 20 and 21 of the Personal Data Protection Law require that all processing of personal data be conducted on a valid legal basis and in accordance with a clear processing purpose.

In the context of employment relationships, corporations act as controllers of workers' personal data. Therefore, corporations are bound by the principles of personal data protection as stipulated in Articles 16 and 18 of the Personal Data Protection Law, including the principles of purpose limitation, data minimization, accuracy, security, and accountability. Supervision of workers outside of working hours that results in excessive, irrelevant, or unjustified processing of personal data potentially violates these provisions.

Normatively (*das sollen*), worker supervision is only justified as long as it is conducted within the scope of the employment relationship and does not violate the right to privacy and personal data protection. However, empirically (*das sein*), the practice of monitoring workers outside of working hours is still found, carried out as a corporate policy without clear regulations regarding the limits of authority and mechanisms for protecting personal data. This gap between labor law norms, the ITE Law, and the Personal Data Protection Law, and actual supervisory practices gives rise to serious legal issues.

If the practice of monitoring workers outside of working hours is carried out systematically and structured as a corporate policy and results in a violation of personal data protection, then legal issues regarding corporate criminal liability arise. In this context, corporations are no longer viewed merely as administrative entities but as subjects of criminal law that can be held accountable for the violations they cause.

Based on the above description, this research is important to comprehensively examine the limits of corporate authority in supervising workers outside working hours by referring to labor law norms, the ITE Law, and the Personal Data Protection Law, as well as to analyze the construction of corporate criminal liability for supervisory practices that result in violations of personal data protection.

Based on this, the formulation of the research problem is:

1. What are the limits of corporate supervisory authority outside working hours according to employment law?

2. How do this surveillance practices potentially deviate from the ITE Law and the Personal Data Protection Law?
3. How is the construction of corporate criminal liability for supervisory practices outside of working hours?

2. METHOD

This research is a normative legal study using a statutory and conceptual approach. The statutory approach is used to analyze the limits of corporate supervisory authority based on the provisions of the Employment Law, the Electronic Information and Transactions Law, and the Personal Data Protection Law. The conceptual approach is used to analyze the concept of corporate criminal liability and the protection of workers' privacy rights.

Primary legal materials include: Law Number 13 of 2003 concerning Manpower, Law Number 11 of 2008, in conjunction with Law Number 19 of 2016 concerning ITE, Law Number 27 of 2022 concerning Personal Data Protection

Secondary legal materials include literature on corporate criminal law, personal data protection, and employment law. The analysis was conducted qualitatively through systematic interpretation of articles governing supervisory authority, electronic data access, and personal data processing to assess potential deviations from statutory law by corporate practices.

3. RESULTS AND DISCUSSION

This research is not limited to a specific geographic location, but rather focuses on the socio-legal context of employment relations in Indonesia, specifically the implementation of after-hours worker supervision implemented through technology-based corporate policies. Therefore, the term "research location" in this study refers to the interaction between company supervision policies, the use of detection devices, and workers' private lives outside of work hours.

Based on empirical data obtained from informants, off-hours surveillance practices are conducted through the use of technology-based detection devices that are mandatory for workers. These devices are not only used during work hours but must also be worn after workers return home, particularly before and during their sleep breaks. The official purpose of these devices is to serve as a control aid to monitor workers' physical condition and accumulate rest hours, which are then used as a basis for assessing workers' readiness to return to work.

In practice, these detection devices work by recording certain biological indicators, such as heart rate and body activity, which are automatically recorded in the company's monitoring system. The data generated by these devices is used as a parameter to assess the quality and quantity of workers' rest time, without any clear separation between work time and private time.

Scheme for Using Detection Tools Based on Shift Work Patterns The use of these detection tools is integrated with shift-based work patterns, both in two-shift and three-shift systems, with the general pattern being that the tools remain in use after work hours end until workers take a sleep break.

1. Two-Shift Work Pattern

In a two-shift work pattern, the use of detection equipment takes place as follows:

a. Shift 1

- Working hours: 06.30 – 18.00
- After work, workers return to their residences and are still required to wear detection equipment.

- Before bedtime, detection devices are used to monitor the biological condition of workers during nighttime sleep.
- Data accumulation: biological activity during night rest is recorded and counted as workers' rest hours in the monitoring system.

b. Shift 2

- Working hours: 17.30 – 07.00
- After work, workers come home in the morning and wear the detection device before taking a nap.
- Approaching sleep rest: biological conditions during naps are still monitored.
- Accumulated data: the afternoon break is treated as equivalent to the night break and is counted as rest hours.

In both schemes, the use of the detection device does not stop at the end of working hours, but continues automatically into the worker's rest phase.

2. Three Shift Work Pattern

In a three-shift work pattern, the detection device usage scheme is adjusted to the rest time of each shift, but the monitoring principle remains the same.

a. Shift 1

- Working hours: 06.30 – 15.00
- After work, workers wear detection devices before going to bed at night.
- Data accumulation: night breaks are recorded as workers' rest hours.

b. Shift 2

- Working hours: 14.30 – 23.00
- After work, workers use detection devices before going to bed at night or in the early morning.
- Data accumulation: rest time is recorded and calculated in the monitoring system.

c. Shift 3

- Working hours: 22.30 – 07.00
- After work, workers use detection devices before going to bed in the morning or afternoon.
- Data accumulation: The lunch break is still treated as a monitored break.

1. Limits of Corporate Supervisory Authority According to Employment Law

Employers' supervisory authority stems from the employment relationship, which is based on the elements of work, wages, and orders. The order element legitimizes supervision, but is normatively limited by the performance of the work. Article 77 of the Manpower Law regulates working hours, while Article 79 regulates workers' rest rights. These provisions indicate that work obligations are only inherent in specific working hours.

The legal implication is that outside of working hours, workers are in a private space and not directly subordinate to the employer. Therefore, supervision outside of working hours has no normative basis in labor law. If corporations continue to supervise workers' activities outside of working hours, such action constitutes an expansion of authority that goes beyond the employment relationship.

This expansion constitutes a deviation from the limits of authority established by law, as the employment relationship does not provide legitimacy for employers to control workers' private lives. Therefore, the practice of monitoring outside of working hours contradicts the principle of limiting authority under labor law.

2. Deviations in Supervisory Practices against the ITE Law

Surveillance of workers outside of working hours is generally conducted through electronic systems such as location tracking, device monitoring, or digital activity monitoring. Under the ITE Law, the use of electronic systems must be lawful and not violate the rights of others.

Article 30 of the ITE Law prohibits unauthorized access to another person's electronic systems. If a corporation accesses an employee's data or electronic activity outside of working hours without a legal basis or valid consent, such action could potentially constitute unauthorized access. Article 46 of the ITE Law stipulates criminal sanctions for such violations.

Thus, electronic surveillance of workers outside of working hours may constitute a violation of the provisions of the ITE Law because it involves access to personal data or activities that are no longer within the context of an employment relationship. This violation demonstrates that corporate surveillance practices have exceeded the legal legitimacy of electronic systems.

3. Deviations from the Principles of Personal Data Protection

Surveillance of workers outside of working hours almost always involves the processing of personal data, such as location, digital activity, or social behavior. The Personal Data Protection Law stipulates that data processing must have a valid legal basis and a clear purpose (Articles 20 and 21). Furthermore, Articles 16 and 18 establish the principles of purpose limitation and data minimization.

Supervision outside of working hours generally has no legal basis because it is not directly related to the performance of work. Furthermore, processing workers' personal data outside of the work context goes beyond the purpose of the employment relationship. Therefore, this practice constitutes unlawful processing of personal data, as prohibited by Article 65 of the Personal Data Protection Law.

If the data processing is carried out by a corporation as a matter of company policy, the provisions on corporate criminal liability under Article 69 of the Personal Data Protection Law apply. Sanctions can include fines, confiscation of profits, termination of activities, or dissolution of the corporation.

Thus, monitoring workers outside working hours constitutes a deviation from the personal data protection regime as it involves processing data without a valid legal basis and goes beyond the purposes of processing.

4. Construction of Corporate Criminal Liability

Modern criminal law recognizes corporations as subjects of criminal law responsible for acts committed within the scope of business activities or organizational policies. Corporate wrongdoing can stem from policies, systems, or organizational culture that allow violations to occur.

In the context of supervision of workers outside working hours, the elements of corporate criminal liability are fulfilled if:

1. Supervision is carried out as a company policy or system.
2. There is processing of personal data without a valid legal basis.
3. There was a violation of the ITE Law or the Personal Data Protection Law.
4. Practices carried out in the interests of the corporation;
5. There is a functional relationship between the perpetrator and the corporation.

If these elements are met, the corporation can be held criminally liable. Therefore, the practice of monitoring workers outside of working hours is not merely an

administrative irregularity, but a potential corporate crime under the personal data protection and electronic systems regime.

4. CONCLUSION

Based on the results of research and discussion regarding *Corporate Criminal Liability for Off-Hour Worker Surveillance Practices that Result in Personal Data Protection Violations*, the conclusion of this research is as follows:

1. The practice of monitoring workers outside working hours through the use of technology-based detection tools is not entirely in line with the principles of employment law.

The research results show that continuous supervision conducted outside of working hours, including during workers' rest and sleep periods, exceeds the employer's authority within the employment relationship. From a labor law perspective, supervisory authority should be limited to the implementation of work during working hours, so supervision outside of working hours has the potential to interfere with workers' rights to rest and privacy.

2. The use of detection devices that record workers' biological data has the potential to violate the principle of personal data protection.

Biological data recorded through detection devices constitutes sensitive personal data. This research found that this data processing was carried out without explicit, specific, and transparent consent and involved workers' activities outside of employment relationships. This situation demonstrates a violation of the principles of legality, clear purpose, and proportionality in personal data protection.

3. The practice of electronic system-based worker surveillance has cross-regime legal implications.

Supervision conducted through electronic systems places corporations, as the providers of electronic systems, under a legal obligation to protect employee data and privacy. When these systems are used intrusively and beyond their legitimate purposes, these practices potentially violate legal provisions in the areas of information technology and personal data protection.

4. The practice of supervising workers outside of working hours has the potential to give rise to corporate criminal liability.

This study concludes that if supervision is carried out as a structural and sustainable corporate policy or system, and has an impact on violations of workers' privacy rights and personal data protection, then criminal responsibility can be imposed on the corporation as a subject of criminal law.

5. SUGGESTIONS

Based on these conclusions, and taking into account the theoretical and practical benefits of this research, the researcher makes the following suggestions:

1. Suggestions for Policy Makers

Policymakers need to clarify and strengthen regulations regarding the limits of worker supervision authority, particularly those conducted outside of working hours and using monitoring technology. These regulations need to be explicitly aligned with labor law, personal data protection law, and information technology regulations to avoid legal gaps or overlapping norms.

2. Advice for Corporations and Technology Users

Corporations are advised to exercise caution when using surveillance technology on workers. Any form of surveillance should be limited to legitimate work interests,

conducted proportionately, and accompanied by clear and transparent employee consent, particularly when monitoring occurs outside of working hours and involves sensitive personal data.

3. Recommendations for Law Enforcement Officials and Regulators

Law enforcement officials and regulatory agencies need to improve their understanding and oversight of technology-based worker surveillance practices. Consistent law enforcement is necessary to prevent personal data protection violations and to ensure that corporate criminal liability can be effectively applied when violations are discovered.

4. Suggestions for Further Researchers

Further research is recommended to further examine the practice of technology-based worker supervision using a comparative legal approach or specific sectoral case studies, in order to enrich academic perspectives and provide more specific recommendations for legal development in the fields of employment and personal data protection.

5. ACKNOWLEDGMENTS

Our thanks go to:

1. Prof. Dr. Mustofa Kamil, Dipl.RSI., M.Pd. as the Chancellor of Syekh-Yusuf Islamic University (UNIS), for all the academic policies and facilities provided during the author's education at UNIS.
2. Dr. Siti Humulhaer, S.H., M.H., as Supervisor I and Head of the Master of Law Study Program, Syekh-Yusuf Islamic University (UNIS), for her patience, scientific guidance, and careful direction in the preparation of this thesis.
3. All Lecturers of the Postgraduate Program in Law at Syekh-Yusuf Islamic University (UNIS), who have provided knowledge, insight, and academic inspiration during the lecture period.

6. BIBLIOGRAPHY

Book

- Asshiddiqie, J. (2016). *Pengantar Ilmu Hukum Tata Negara*. Jakarta: Rajawali Pers.
- Barda Nawawi Arief. (2018). *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana*. Jakarta: Kencana.
- Budhijanto, D. (2019). *Hukum Telekomunikasi, Penyiaran, dan Teknologi Informasi*. Bandung: Refika Aditama.
- Huda, N. (2017). *Hukum Ketenagakerjaan Indonesia*. Jakarta: RajaGrafindo Persada.
- Marzuki, P. M. (2021). *Penelitian Hukum*. Jakarta: Kencana.
- Mertokusumo, S. (2019). *Mengenal Hukum: Suatu Pengantar*. Yogyakarta: Cahaya Atma Pustaka.
- Moeljatno. (2018). *Asas-Asas Hukum Pidana*. Jakarta: Rineka Cipta.
- Sutedi, A. (2022). *Hukum Perlindungan Data Pribadi*. Jakarta: Sinar Grafika.
- Widodo, P. (2020). *Hukum Pidana Korporasi*. Jakarta: Prenadamedia Group.

Scientific Journal

- Aprilia, R., & Nugroho, S. (2021). Perlindungan data pribadi pekerja dalam penggunaan teknologi pengawasan digital. *Jurnal Hukum IUS QUIA IUSTUM*, 28(2), 245–268.
- Handayani, I. G. A. K. R. (2022). Pertanggungjawaban pidana korporasi dalam pelanggaran perlindungan data pribadi. *Jurnal Legislasi Indonesia*, 19(3), 389–406.
- Kusumaatmadja, M., & Sidharta. (2020). Perlindungan hak privasi dalam hubungan industrial modern. *Jurnal Hukum & Pembangunan*, 50(4), 712–735.

- Pratama, R. A. (2023). Pengawasan pekerja berbasis teknologi dan implikasi hukum ketenagakerjaan. *Jurnal Ilmu Hukum*, 12(1), 55–74.
- Sari, D. P. (2021). Sistem elektronik dan perlindungan data pribadi dalam hukum Indonesia. *Jurnal RechtsVinding*, 10(2), 181–199.

Legislation

Indonesia. The 1945 Constitution of the Republic of Indonesia.

Indonesia. Law Number 13 of 2003 concerning Manpower.

Indonesia. Law Number 11 of 2008 concerning Electronic Information and Transactions.

Indonesia. Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions.