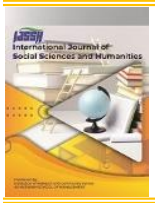

International Journal of Social Sciences and Humanities
Vol. 2 No. 3, Oktober 2024, pages: 94-98
e-ISSN: 2985-6469
https://doi.org/10.55681/ijssh.v2i2.1504

Legal Protection For Employees Who Are Harmed By Data Misuse By The Company

M. Alfitra Gita Armanda[a]*, Krisnadi Nasution[b]

**Corresponding author email: alfitra8888@gmail.com*

Article History

Manuscript submitted:
18 Oktober 2024
Manuscript revised:
20 Oktober 2024
Accepted for publication:
28 Oktober 2024

Keywords
Personal data, employees, company

Abstract

The purpose of this study is to find out how to protect the law for employees who are harmed by the misuse of personal data by the company. This study uses a type of normative juridical research using a statutory approach and a conceptual approach. The development of the times that has led to the development of technology and information systems has caused a lot of data misuse by the public. Companies, in their day-to-day operations, collect and process employee data for a variety of purposes, from personnel administration, performance appraisals, to strategic planning. However, the use of this data often poses a risk of misuse. Misuse of data can take many forms, including but not limited to unauthorized disclosure of personal data, use of data for unauthorized purposes, and disregard for adequate security measures. Misuse of data by companies can take many forms, such as unauthorized dissemination of personal information, use of data for unauthorized purposes, or neglect of data security that leads to leaks. The consequences of this abuse can include financial losses, reputational damage, and psychological impacts for affected employees. The results of this study show that the legal steps that can be taken by employees in dealing with data breaches or misuse reflect the importance of legal protection in safeguarding individual rights. By providing a channel for employees to report violations and sue for damages, the law creates a mechanism that encourages companies to take responsibility and maintain the privacy of employee data.

Contents

[a] Universitas 17 Agustus 1945 Surabaya, Indonesia
[b] Universitas 17 Agustus 1945 Surabaya, Indonesia

Introduction

In the midst of the rapid development of information and communication technology, personal data has become one of the most valuable assets in the business world. This data includes information relating to individuals, including employees, which includes personal data, employment history, performance records, and other sensitive information. With digitalization becoming more widespread, the management and protection of personal data is very important for companie(Lubis and Susanto 2019).

In today's digital era, data is one of the most important assets for companies. Data includes not only information about customers, but also sensitive internal information related to employees, such as personal data, employment history, and performance records. The management and protection of this data is crucial because mistakes or misuse can have a serious impact on both employees and the company(Koto and Hanifah 2023).

Companies, in their day-to-day operations, collect and process employee data for a variety of purposes, from personnel administration, performance appraisals, to strategic planning[c]. However, the use of this data often poses a risk of misuse. Misuse of data can take many forms, including but not limited to unauthorized disclosure of personal data, use of data for unauthorized purposes, and disregard for adequate security measures. Misuse of data by companies can take many forms, such as unauthorized dissemination of personal information, use of data for unauthorized purposes, or neglect of data security that leads to leaks. The consequences of this abuse can include financial losses, reputational damage, and psychological impacts for affected employees (Johan, Lina, and Mustofa 2023).

In many jurisdictions, including Indonesia, there are various regulations and laws governing the protection of personal data. In Indonesia, Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) is the main basis for regulating the management and protection of personal data. However, while such regulations exist, their implementation and enforcement are often challenging, especially in cases involving data misuse by companies against employees (Nursalim and Suryono 2021).

Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) provides a comprehensive legal framework related to the collection, processing, and storage of personal data. In the context of the misuse of employee data by companies, there are several important articles in this law that are often violated.

One of the main aspects violated in cases of data misuse is the basic principles of data processing regulated in Article 5 of the PDP Law. This article stipulates that the processing of personal data must be carried out fairly, lawfully, and for specific, clear, and legitimate purposes. Misuse of employee data, such as using their data for unrelated interests or without consent, is clearly contrary to these principles.

In addition, Article 12 of the PDP Law provides special protection for data subjects, in this case employees, by stipulating their rights regarding personal data. Employees have the right to access their data, correct errors in the data, delete irrelevant data, and object to undesirable data processing. If a company ignores these rights or does not provide a mechanism to fulfill them, then the company can be considered to be in violation of the PDP Law.

Furthermore, Article 18 of the PDP Law requires companies to provide clear and transparent information to data subjects regarding the processing of their personal data. Failure to provide accurate, complete information, or provide misleading information to employees about how their data is used may be considered a violation of the provisions of the PDP Law (Pakpahan, Luh Ayu Mondrisa Dwipayana, and Setiyono 2020).

Companies are also required to maintain the security of personal data in accordance with the provisions of Article 46 of the PDP Law. This article stipulates that companies must implement adequate security measures to protect employees' personal data from various threats, including illegal access, leaks, or hacking. If the company does not implement appropriate security systems, then this can be considered as negligence and a violation of their obligations.

Materials and Methods

In this study, the author uses a type of normative juridical research using a statutory approach and a conceptual approach. The legal materials used are primary legal materials and secondary legal materials (Marzuki 2022).

Results and Discussions

Legal protection for employees who are harmed by data misuse by the company

Legal protection for employees is one of the fundamental aspects in industrial relations between workers and companies. This protection not only serves to maintain the welfare of employees, but also to create a fair, safe, and productive work environment. In practice, this legal protection covers various dimensions involving basic employee rights, such as the right to a decent wage, protection from discriminatory treatment, the right to social security and health, and occupational safety and health (K3) guarantees (Suandi and Martinesya 2021).

First, the basic rights of employees include things such as a minimum wage that is in accordance with the standards set out in laws and regulations, reasonable working hours, and the right to leave. For example, in accordance with Law No. 13 of 2003 concerning Manpower and its derivative regulations, companies are obliged to pay decent wages and in accordance with regional provisions. In addition, employees are also entitled to rest time, annual leave, maternity leave for women, and other benefits regulated by company regulations and collective bargaining agreements (Fungsi 2014).

Second, protection against discriminatory acts is also important in employment relations. Discrimination based on race, religion, gender, or social status constitutes a serious violation of human rights. In this context, the labor law provides protection to employees from all forms of discrimination, both in the process of recruitment, payroll, promotion, and termination of employment (PHK). Equality in the workplace is a principle that must be upheld by companies to create harmonious working relationships (Nita and Susilo 2020).

Third, ensuring work safety is a crucial element in maintaining the physical and mental well-being of employees. In risky work environments, such as the manufacturing or construction industry, companies are required to provide personal protective equipment (PPE) and comply with occupational safety standards. This is regulated in Law No. 1 of 1970 concerning Occupational Safety, which requires companies to ensure that the workplace is free from potential hazards that could threaten the safety and health of workers. Violations of occupational safety rules not only have a bad impact on workers, but can also result in severe sanctions for the company (Iswaningsih, Budiartha, and Ujianti 2021).

In addition, social security is also an important aspect of legal protection for employees. The government, through BPJS Employment and BPJS Kesehatan, requires every company to register employees in the social security program. This program includes old-age insurance, work accident insurance, health insurance, and pension insurance. The purpose of the program is to provide protection for employees from social and economic risks that may occur during their employment or after retirement (Nuryawan 2020).

In the digital era, the protection of employees' personal data is also the main highlight. With the increasing use of information technology in the work environment, employee personal data such as financial information, health, and other personal data are often collected and managed by companies. However, the management of this data must be carried out in accordance with applicable regulations, such as the newly passed Personal Data Protection Act, which regulates employees' rights to the privacy of their data as well as the company's obligation to protect such data from misuse.

In today's digital era, employee personal data is one of the important aspects that must be protected by companies. Improper data management or data misuse by the company can cause significant losses to employees, both materially and immaterially. In this context, legal protection for employees who are harmed by data misuse has become an increasingly relevant issue, considering the importance of maintaining privacy and security of personal information (Thalib and Maswari 2021).

Misuse of employee data can occur in various forms, such as unauthorized disclosure of personal data to third parties, utilization of data for commercial purposes without the employee's knowledge, and use of data that violates privacy, such as accessing financial or health information without consent. These actions have a very significant impact, especially when sensitive information such as health status or financial data is leaked.

Employees who are harmed by this data misuse can suffer losses in the form of loss of privacy, damage to reputation, and real economic losses (Pertiwi et al. 2022).

For example, financial information leaks can be exploited by irresponsible parties for fraud or identity theft purposes, which can ultimately cost employees financially. In addition, violations of health privacy can result in social stigma that harms employees in the workplace and in their environment (Kesuma, Budiartha, and Wesna 2021). This analysis shows that companies have a great responsibility in maintaining the confidentiality and integrity of employee data, as well as implementing strict security systems to prevent misuse. Without adequate protection mechanisms, the risk of losses for employees is increasing, which in turn can have a negative impact on the working relationship and employee trust in the company. Therefore, the implementation of strict and transparent data protection policies is indispensable to maintain a balance between the interests of the company and the rights of employees.

Companies are required to implement strict security measures in managing employee data. The company's responsibilities include implementing an information security system, granting limited access to the authorities, and ensuring that the use of data always receives approval from employees in accordance with the principles of personal data protection. In addition, companies must also be transparent about data collection and use, and must provide clear information to employees regarding how their data will be used (Nursantih and Ratnawati 2023).

Employees have certain rights related to the protection of their personal data under the PDP Law. Some of these rights include the right to know the management of their personal data, the right to give or withdraw consent to the use of data, and the right to request the deletion or correction of inappropriate personal data (Nursantih and Ratnawati 2023).

In the event of a data breach or misuse, employees have several legal steps that can be taken to protect their rights. The first step is to report the violation to the appropriate authority, such as the Information Commission or the Ministry of Communication and Informatics. Through this report, the authority can conduct an investigation and take the necessary action against the company in question. This process is important to ensure that the company complies with existing data protection regulations and is responsible for actions that harm employees.

The second step that employees can take is to file a civil lawsuit against the company to demand compensation for losses incurred due to data misuse. In this context, employees have the right to seek compensation for material losses, such as financial losses experienced due to data leaks, as well as immaterial losses, such as stress or reputational damage. This process often involves gathering evidence and strong arguments to support the employee's claims in court (Kesuma et al. 2021).

In addition, if the misuse of data falls into the category of criminal offenses in accordance with the Personal Data Protection Law (PDP Law), employees can also sue the company criminally. This action can involve prosecuting individuals or parties in the company who are responsible for violations of the law. In these cases, employees can work closely with law enforcement officials to gather evidence and draft reports that support criminal charges (Thalib and Maswari 2021).

The legal steps that employees can take in dealing with data breaches or misuse reflect the importance of legal protection in safeguarding individual rights. By providing a channel for employees to report violations and sue for damages, the law creates a mechanism that encourages companies to take responsibility and maintain the privacy of employee data. However, there are some challenges that employees may face in going through this process, such as the need for strong evidence and potential intimidation from the company. Therefore, education about employee rights and support from organizations that advocate for data protection is essential to help employees deal with this situation. On the other hand, companies need to increase awareness and compliance with data protection regulations in order to avoid potential legal disputes that are detrimental to both parties.

Conclusion

The legal steps that employees can take in dealing with data breaches or misuse reflect the importance of legal protection in safeguarding individual rights. By providing a channel for employees to report violations and sue for damages, the law creates a mechanism that encourages companies to take responsibility and maintain the privacy of employee data. However, there are some challenges that employees may face in going

through this process, such as the need for strong evidence and potential intimidation from the company. Therefore, education about employee rights and support from organizations that advocate for data protection is essential to help employees deal with this situation. On the other hand, companies need to increase awareness and compliance with data protection regulations in order to avoid potential legal disputes that are detrimental to both parties.

References

Fungsi, Kedudukan D. A. N. 2014. "Kedudukan Dan Fungsi Perjanjian Kerja Bersama Dalam Pelaksanaan Hubungan Industrial Berdasarkan Undang-Undang Nomor 13 Tahun 2003." *Jurnal Ilmiah Hukum Dirgantara* 7(1):111–21. doi: 10.35968/jh.v7i1.126.

Iswaningsih, May Linda, I. Nyoman Putu Budiartha, and Ni Made Puspasutari Ujianti. 2021. "Perlindungan Hukum Terhadap Tenaga Kerja Lokal Dalam Undang-Undang Nomor 11 Tahun 2020 Tentang Omnibus Law Cipta Kerja." *Jurnal Preferensi Hukum* 2(3):478–84. doi: 10.22225/jph.2.3.3986.478-484.

Johan, A., R. Lina, and M. E. Mustofa. 2023. "Perlindungan Hukum Terhadap Hak Pekerja Dalam Perusahaan Melakukan Coorporate Action Merger Dan Akuisisi." *Prosiding …* (2):13–24.

Kesuma, A. A. Ngurah Deddy Hendra, I. Nyoman Putu Budiartha, and Puru Ayu Sriasih Wesna. 2021. "Perlindungan Hukum Terhadap Keamanan Data Pribadi Konsumen Teknologi Finansial Dalam Transaksi Elektronik." *Jurnal Preferensi Hukum* 2(2). Hlm. 411–16. doi: 10.22225/jph.2.2.3350.411-416.

Koto, Ismail, and Ida Hanifah. 2023. "Aspek Hukum Pelaksanaan Pekerjaan Pokok Oleh Tenaga Kerja Outsourcing Di Indonesia." *Legalitas: Jurnal Hukum* 14(2):193. doi: 10.33087/legalitas.v14i2.333.

Lubis, Efridani, and Haryogis Susanto. 2019. "Penerapan Good Corporate Governance Di Pasar Modal Sebagai Upaya Melindungi Investor." *Jurnal Hukum Dan Bisnis (Selisik)* 5(1):48–76. doi: 10.35814/selisik.v5i1.1285.

Marzuki, Peter Mahmud. 2022. *Penelitian Hukum*. Jakarta: Kencana Prenada Media Group.

Nita, Surya, and Joko Susilo. 2020. "Peranan Serikat Pekerja Dalam Membentuk Perjanjian Kerja Bersama Sebagai Hubungan Kerja Ideal Bagi Pekerja Dengan Pengusaha." *De'Rechtsstaat* 6(2):143–52. doi: 10.30997/jhd.v6i2.2819.

Nursalim, Chairunnisa Ramadhani Putri, and Leli Joko Suryono. 2021. "Perlindungan Hukum Tenaga Kerja Pada Perjanjian Kerja Outsourcing." *Media of Law and Sharia* 2(1):47–62. doi: 10.18196/mls.v2i1.11478.

Nursantih, Nadia, and Elfrida Ratnawati. 2023. "Pengawasan Ojk Atas Data Pribadi Konsumen Pada Perusahaan Peer To Peer Lending." *Unes Law Review* 5(4):1564–79.

Nuryawan, I. Dewa Gede Oka. 2020. "Rekonstruksi Perjanjian Kerja Bersama Dalam Undang-Undang Nomor 13 Tahun 2003 Tentang Ketenagakerjaan." *Jurnal Analisis Hukum* 1(2):255. doi: 10.38043/jah.v1i2.415.

Pakpahan, Hatarto, Ni Luh Ayu Mondrisa Dwipayana, and Setiyono. 2020. "Cyberbullying Di Media Sosial." *Bhirawa Law Journal* 1(2):63–70.

Pertiwi, Endah, Dzikra Delvina Nuraldini, Gilang Tri Buana, and Amos Arthacerses. 2022. "Analisis Yuridis Terhadap Penyalahgunaan Data Pribadi Pengguna Media Sosial." *Jurnal Rechten : Riset Hukum Dan Hak Asasi Manusia* 3(3):10–16. doi: 10.52005/rechten.v3i3.65.

Suandi, and Sefa Martinesya. 2021. "Tanggung Jawab Pemerintah Terhadap Hak Konstitusional Tenaga Kerja Outsourcing." *Jurnal Cakrawala Ilmiah* 1(4):877–88.

Thalib, Emmy Febriani, and Ketut Laksmi Maswari. 2021. "Perlindungan Hukum Terhadap Data Pribadi Perusahaan Akibat Penyalahgunaan Data Digital Oleh Karyawan Perusahaan." *Prosiding Seminar Nasional Fakultas Hukum Universitas Mahasaraswati Denpasar 2020* Vol 1(No 1):55–66.