Employee Privacy Rights In India
written by King Stubb & Kasiva | March 14, 2023

Privacy is the state of being left alone and free from unauthorized observation and attention. Article 21 of the Constitution of India guarantees the 'Right to Privacy' as a part of the 'Right to Life'. The right to privacy was acknowledged in the case of *Govind v. State of Madhya Pradesh*, as a part of the wider right guaranteed under Art. 19(a), (d), and 21. This case highlighted that the right to privacy is a fundamental right, but it must be subject to limitations based on compelling public interest.

Employees have the right to some degree of personal space as well as the right to keep personal information about themselves, concealed and the right to privacy about their work-related actions and personal information, but more frequently than expected, company policies override these rights. Employers can monitor a variety of workplace activities with technology. They may track the "digital footprints" of their workers using variety of technologies to learn more about how they behave. An employee's workplace conversations may be observed and read by the employer, save for the limitations as may be prescribed under applicable laws or rules of the organisation.

Overview of Employee Privacy Rights

Employee privacy rights limit how extensively an employer can search an employee’s data and belongings; monitor their actions, speech, or correspondence; and know about their personal lives. An employee privacy policy is documentation specifying an organization's rules and procedures for using the personal information of employees.

There are legislations controlling conditions of work, non-discrimination, maternity laws, payment of wages, etc., in terms of employee rights. However, the fact that there is no specific legislation governing the privacy rights of workers, necessitates that employers lay down specific guidelines in this regard.

Legal Framework for Protecting Employee Privacy Rights

The privacy rights of workers/employees in our country can be drawn from different legislations that either directly or indirectly, provide such protection in the absence of a specific data protection law for workplaces in India. The following are some of the laws that address the subject:

1. A comprehensive digital data protection law in India is being attempted with the Digital Personal Data Protection Bill, 2022(DPDP Bill), (yet to be brought into force), which will regulate the processing of digital personal data by safeguarding the right to privacy of individuals.
2. The Information Technology Act of 2000 and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Information) Rules of 2011 (the "IT Rules") are currently the principal laws that deal with data protection. As per IT Act and the IT Rules, "personal information" and "sensitive personal data or information" -specifically, information related to passwords, and financial information, such as bank account, credit card, debit card, or other payment instrument details, physical, physiological, and mental health conditions, sexual orientation, medical records and histories, and biometric information - are what are sought to be protected most. The IT Act and the IT Rules are the legal frameworks the government has established for data protection and privacy through the following relevant sections: -
3. Section 43 (a),(b) and (i): any person who either, (a) accesses a computer, computer system or computer network, (b) downloads copies, or extracts any data, computer data base or information from such computer, computer system or computer network which includes information or data held or stored in any removable storage medium; (c) steals, conceals, destroys or alters or causes any person to steal, conceal, destroy or alterany computer source code used for a computer resource; with the intent to cause harm and without the owner’s consent (or the consent of any other person who is in charge of the computer/computer system/computer network) shall be held liable and be required under this section to pay damages of not more than Rs One Crore to the person affected.
4. Section 43A: In the event that a body corporate negligently fails to implement and maintain reasonable security practises and procedures and causes wrongful loss or wrongful gain to any person while handling sensitive personal data or information in a computer resource that it owns, controls, or operates, such body corporate shall be liable to pay damages by way of compensation, which shall not exceed Rupees Five Crores.
5. Section 66C: Anybody who uses another person's electronic signature, password, or any other unique identification feature dishonestly or

fraudulently maybe punished with imprisonment of up to three years and a fine of up to INR 1,00,000 in addition to their punishment.

6. Section 72A: If someone, including an intermediary, discloses information about another person without that person's consent or in violation of a legal contract while performing services under the terms of a legal contract, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain, they maybe punished with imprisonment for a term that may extend to three years or with fine extending to five lakhs or both.

Common Privacy Issues in the Workplace

There are two main privacy issues through which Employee privacy is compromised, by employers –

1. Collection of Sensitive Personal Data or information (SPDI): Companies gather SPDI from their workers for a variety of objectives, including the hiring process, record retention, employee assessments, and other legitimate business needs. The confidentiality of the workers is jeopardised when this information is gathered and then disclosed or provided to third parties. According to Rule 5 of the IT Rules, no body corporate or person acting on its behalf may collect sensitive personal data or information unless;

1. the information is used for a legitimate purpose related to one of the body corporate's functions or activities, and
2. the collection of such data is deemed necessary for that purpose.

3. Employee Surveillance: Employees' actions are frequently observed by employers. Records of Telephonic communication and computer surfing are kept a tab off, which invades employee privacy. When an employee joins a company, he agrees to provide information that is important for the work and not any other personal information.

To make the right to privacy meaningful, it is the duty of the state to put in place a data protection framework that, while protecting employees from dangers to informational privacy originating from company policies, serves the common good.

Impact of Technology on Employee Privacy Rights

Increased efficiency and order in daily life are now largely owing to technological advancements like the wide variety of electronic communications, computer-based document generation and storage, and other countless futuristic breakthroughs. Employees are frequently expected to use electronic resources provided by their company in the contemporary office, including cell phones/laptops/email. In a time when GPS tracking is a reality, Companies have a strong commercial reason for keeping an eye on how their employees' travel data and how they use corporate resources. This might involve gathering data from personal e-mail, chat, or social media accounts that employees have accessed while using company equipment or technology.

In the absence of a well-defined data protection law/policy, it is necessary that the companies lay down specific guidelines in compliance with applicable laws as tohow an employee's right to a reasonable expectation of privacy in their communications should be balanced with an employer's right to access such data, for whatever reason there might be.

Conclusion

A data protection law for employee privacy is the need of the hour. Even though there are specific laws for employee benefits, however, to protect their personal data and private space, it is important to have a defined/specific data protection law for workplaces.

Additionally, employee data privacy can be ensured through the following ways –

- Companies must collect limited employee data, only as much as needed for business purposes.
- In case a company requires additional data from an employee which may be a part of sensitive and personal information, specific consent of the employee must be taken for the same.
- Employees must enter into a well-documented privacy policy upon joining, which must also be posted on the employer's website.
- The flaws in the information provided should be permitted to be revised or fixed by the employees.
- Employers are required to uphold appropriate safeguards for SPDI, which employees provide them access to.

FAQs

What are the legal frameworks governing employee privacy rights in India?

There is no specific law governing employee privacy rights in India. However, the privacy rights of workers/employees in our country can be drawn from different legislations that either directly or indirectly, provide such protection in the absence of a specific data protection law in India. For instance,

1. The IT act, 2000 protects the information of an organisation as well as an individual, be it an employee, and prescribes punishment for the offences with a hefty fine.

2. A comprehensive digital data protection law in India is being attempted with the Digital Personal Data Protection Bill, 2022 (DPDP Bill).

What are the employer’s responsibilities to protect employee privacy?

The employer must ensure to draft a well-documented employee policy in addition to taking prior and specific consent of the employee, before asking for personal and sensitive data. Additionally, the employer must ensure to use appropriate procedures to protect the employee’s information in every possible way.

What types of personal information are protected under Indian laws?

Information related to passwords, financial information, such as bank account, credit card, debit card, or other payment instrument details, physical, physiological, and mental health conditions, sexual orientation, medical records and histories, and biometric information are specifically protected by the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011.

King Stubb & Kasiva,
Advocates & Attorneys
Click Here to Get in Touch
New Delhi | Mumbai | Bangalore | Chennai | Hyderabad | Mangalore | Pune | Kochi | Kolkata
Tel: +91 11 41032969 | Email: info@ksandk.com