Page 1449 - 1457

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 4 | Issue 2

2021

Need for a Comprehensive Legislation on Employee's Privacy in India: Comparison With U.S and EU Models

PREETHI. A[1] AND NITHIN SATHEESH[2]

ABSTRACT

Laws are always required to cater the needs of both the present and the future technologies. In the present age, there is an increasing magnitude of issues the employees counter at the workplace. A smooth workplace is crucial for both the employers and the employees for a progressive national development. Employee's privacy at workplace is one among the unspoken heads in the privacy regime. If India lacks a sound privacy protection, there would be a massive drawback in its position on the global map. This paper articulates the existing legislation on employee's privacy in U.S, EU and India. Further, it points out the loopholes spotted in the Indian Legislation. Finally, the authors compare different country's models of the employee's privacy regime and suggest the best befitted model for India.

I. INTRODUCTION

Employment law enfolds all the rights and obligations with reference to the employer-employee relationship. This branch of law concerns issues regarding discrimination of employees, unlawful termination, harassment and workplace safety. Employee privacy is a major and indispensible part of this stream.

In today's digital era, privacy has gained an ample paramount after several Supreme Court judgments. The Supreme Court in K. Puttaswamy & Ors V. UOI, has upheld the right to privacy under Article 21 of the Constitution of India. As such, employee's privacy is no less important for a smooth and progressive work environment.

At present, India has no robust legislation covering the employee privacy rights at workplace. This article aims to compare the different models of employee privacy in U.S and E.U. This discussion will scrutinize which country's model would be best suited to India for effective

[1] Author is a student at School of Excellence in Law, TNDALU, India.
[2] Author is an Advocate at Bar council of Tamilnadu and Puducherry, India.

 [ISSN 2581-5369]

privacy legislation.

Employee's Privacy Rights

Employee's privacy rights are the rights available to them to prevent the employer from unlawful disclosure of personal information, monitoring the employee and the extent to which they can know the employee's lives. This topic is clinching more concern nowadays as there is a fast hike in the development of technologies. The prevailing laws are insufficient around the countries to protect the privacy of the employees at the workplace.[3]

II. COMPARATIVE ANALYSIS OF EMPLOYEE'S PRIVACY LAWS IN U.S., EU AND INDIA

1) United States:

In U.S, the workplace privacy of employees is governed not only by the federal statutes and U.S constitution but also by specific laws of the states. Every state stipulates respective law to oversee the surveillance, social media, email, telephone use and physical space of the employees. Only a minimal protection is extended to the private sector employees. Intrusions into the privacy of the public sector employees are brought under the regime of U.S privacy policy.

Legal Framework:

The U.S tort, constitutional laws and contract laws provides a midget level of protection to the employee privacy. The entire legal framework is derived from the federal state laws.

U.S Constitution:

There is no express provision in the U.S Constitution related to the right to privacy. It is created by the First, Fourth and Fifth Amendment. The fourth amendment indicates prohibition of unreasonable search and seizure. ***Boyd V. United States***[4] is the first decision bridging the concepts of privacy and fourth amendment. The prevailing two major federal laws relating to privacy are Privacy Act, 1974 and Electronic Communication Privacy Act (ECPA).

Privacy Act:

The U.S Privacy Act of 1974 prohibits disclosing information that is regarded as personal information kept by the schools, employers, credit bureaus and government agencies unless a

[3] Employee privacy rights: Everything you need to know, Upcounsel (12August 2020), https://www.upcounsel.com/employee-privacy-rights.
[4] Boyd v. United States 116 U.S. 616 (1886), JUSTIA US SUPREME COURT, https://supreme.justia.com/cases/federal/us/116/616/.

courts order prevails. The term "Agency" under the Privacy Act is not restrictive. However, this act is not applicable to private sector unlike the Australian model. The Privacy Act paves way for many public sector employees. However, the act is not best opted to address the privacy issues of the employees at workplace and for the breach of monitoring practices of the employees.

Electronic Communication Privacy Act (ECPA)

The basic federal law that oversees privacy issues of communication is Electronic Communication Privacy Act (ECPA). ECPA prohibits unauthorized access and interception to communication in electronic storage. Anyone, including the employer, who intentionally intercepts the electronic, oral, wire communication, shall be brought under the ambit of the act. ECPA amended the Omnibus Crime Control and Safe Streets Act (Known as the Wiretap Act). The ECPA contains the Wiretap Act and Stored Communication Act (SCA)

Wiretap Act

Wiretap Act prohibits the unauthorized and intentional interception to oral, wire and electronic communication whereas ECA restricts access to electronic communication.

Wiretap provides certain defenses:

- Where the employer is a service provider and has the right to monitor their employees lawfully for business reasons.
- Where the employees has consented to such monitoring and interception.
- When such interception is in the ordinary course of business.

Stored Communication Act (SCA):

Where the wiretap act provides restrictions related to communications in transit, SCA act exclusively deals with the prohibition of access to communication in stored devices.

SCA also contain few exceptions where the employer can escape from the liability. In ***Bohach V. The City of Reno***[5],there was found no breach as the police department had the lawful right to access stored messages of their employees. This falls within the exception of the act.

Intersections

It is a serious issue for the courts to determine whether such intrusion falls under the head of wiretap act or SCA. This determination is important with respect to workplace interception as

[5]Bohach v. City of Reno, 932 F. Supp. 1232 (D. Nev. 1996), JUSTIA US LAW, https://law.justia.com/cases/federal/district-courts/FSupp/932/1232/1397960/.

SCA provides more stringent laws.

Although ECPA governs the privacy of communication, it is flexible than the wire- tapping statutes of the states. States have more stringent laws to protect the privacy. For e.g: Security of communications act of Florida is stricter and more precise than ECPA which prohibits interference into the workplace communication without the consent of the recipient and the sender. Further, it restricts the monitoring framework of the employees without the consent of the employee.

Americans with Disabilities Act (1990)

The ADA act shall be applicable to the employees who employ more than 15 persons. This law primarily requires the employer to protect the medical information sought from the employees. This act shall not only be restricted to Americans with disability, but is open to all the employer's monitoring practice and workplace privacy policies.

ADA is a comprehensive legal framework that protects the employee's personal information which is in the form of medical information. This act prohibits the employer from disclosing the medical information in all forms except for limited legal purposes.[6]

ANALYSIS ON THE U.S EMPLOYEE PRIVACY

As far as U.S is concerned, there is no single guiding principle on the employee privacy at workplace. Even U.S constitution is silent on the subject of privacy. Still, there are different laws enacted by the federal states to protect different sets of information.

In U.S, the concept of privacy can be regarded as a reasonable expectation from the employees at the workplace. The law tries to strike a balance between the employer's business interest and the employee's privacy protection. Invasion into privacy can be possible with proper notified technologies to the employees.

The authors view that USA has to take steps to enact a single guiding principle covering all the provisions relating to privacy in addition to the federal state laws. The law should cover both the public and private sector employees for a better overall work environment.

2) European Union:

Reference for employee's privacy in European Union can be taken from General Data Protection Regulation (GDPR). GDPR came into force with effect from May 25, 2018 replacing the Data Protection Directive (DPD).

[6]Kris Janisch, Do employees have any privacy at work, GovDocs (14 November 2019), https://www.govdocs.com /do-employees-have-any-privacy-at work/

General Data Protection Regulation (GDPR)

GDPR is a regulation which is applicable in EU containing provisions related to privacy and data protection in the European Economic Area (EEA). GDPR shall be applicable not only to the EU member states but also to the other employees outside EU who are working in EU. This data privacy regulation which covers consumers also brings the employees into its ambit. This current regulation requires the data controllers as well as the data protectors to adopt appropriate measures to preserve the privacy protection principles. ***Barbulescu V. Romania***[7] was an important judgment delivered on this subject. The European Court of Human Rights held that the employer's had no right to monitor the communications of the employees at the workplace.

Data Protection Directive (DPD) V. GDPR

GDPR was enacted to encounter all the defects found in the DPD. The term 'Personal data' was redefined in GDPR. GDPR covers all information used either on its own or in connection with another data.

Another vital change brought under GDPR is that data processors are brought under its ambit. Earlier only data controllers were held liable for mishandling the personal data. Now, both data processors and data controllers are responsible for violations.

GDPR proposes stricter timelines and procedures for reporting the breaches. It requires the organizations to report within 72hours to the respective authorities and the individuals.

Under the directive, the EU member states were set free to adopt their own laws. But GDPR is a mandatory compliance for all the states.[8]

Countries backing the GDPR model

The introduction of GDPR in EU has set an example for many of the countries to have an appropriate and acceptable regulation circling the data privacy and protection. Several countries have taken GDPR as a precedent in enacting laws in their respective own countries.

- **Brazil:** Lei Geral de Protecao de Dados(LGPD) has taken GDPR as a model. The enforcement of which is postponed till 2021.
- **Australia:** Amendment to the Australia's Privacy Act with effect from February 2018.

[7]Barbulescu V. Romania (2017) ECHR 742, Croner-I, https://app.croneri.co.uk/law-and-guidance/case-reports/b-rbulescu-v-romania-2017-echr-742.
[8]DPD versus GDPR: Understanding key changes, PrivSec Report(6 March 2018), https://gdpr.report/news/2018/03/06/data-protection-directive-versus-gdpr-understanding-key-changes/.

 [ISSN 2581-5369]

- **USA:** There are no federal laws as such in USA. But the recent California Consumer Privacy Act, 2018(CCPA) has taken GDPR as a model while enacting.
- **Japan:** Japan's Act on Protection of Personal Information was amended in May 2017 in lines with GDPR.
- **South Korea:** South Korea's Personal Information Protection Act which has been in force from 2011 includes many like provisions of GDPR.
- **Thailand:** Thailand's Personal Data Protection Act (PDPA) has similar provisions to GDPR in many ways including the definition part, extraterritoriality and strict penalties.[9]

ANALYSIS ON THE EU EMPLOYEE PRIVACY

The fundamental principle of privacy from the European perspective is that it is a human right. The expectation of privacy for the employees of EU is generally high and there is a need on the part of the employer to protect unlawful interference with the employee's privacy. In EU, there is a single omnibus data protection regulation governing the protection of personal information of the consumers. There is no exclusive law for the employer and employee privacy policy. The liabilities of the employers arrive from the regulation which is also applicable to the consumers.

Earlier DPD had lacunae and was not as expansive as how GDPR works now. It lacked on various parts including the definition part, territorial reach and penalties. However, recently GDPR has been passed overcoming all the loopholes of DPD. GDPR can be said to be on point and a precise regulation directly addressing all the privacy issues.

Several countries have referred GDPR as a model for enacting their own laws. The authors are of the view that GDPR satisfies the maximum needs and requirements for the protection of data and privacy of consumers including the employees.

3) India

The Supreme Court has recently held right to privacy as a fundamental right under Article 21 of the Constitution of India. This judgment has implications on the privacy policies of the employee. In spite of gaining paramount importance and consideration in today's world, India lacks a comprehensive legislation on data security and privacy policy. At present the privacy policies and data security are dealt in the Information Technology Act, 2000 and SPDI Rules,

[9]Dan Simmons, 9 countries with GDPR like Data Privacy Laws, Comforte blog(17 January 2019), https://insights.comforte.com/9-countries-with-gdpr-like-data-privacy-laws.

 [ISSN 2581-5369]

2011.

Information Technology Act, 2000 (IT Act)

Any reference on data privacy and employee privacy has to stem from the Information Technology Act, 2000.

Sec 43-A deals with the protection of 'sensitive personal data or information'.

43A. Compensation for failure to protect data.–Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected.

Explanation –For the purposes of this section,–

(i) body corporate means any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities;

(ii) reasonable security practices and procedures means security practices and procedures designed to protect such information from unauthorised access, damage, use, modification, disclosure or impairment, as may be specified in an agreement between the parties or as may be specified in any law for the time being in force and in the absence of such agreement or any law, such reasonable security practices and procedures, as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit;

(iii) Sensitive personal data or information means such personal information as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit.[10]

The employee's personal information qualifies to be a 'sensitive personal data or information'. Henceforth, the employers are required to maintain reasonable security procedure and practices to protect the employee's data. Failure of which will attract penal consequences.

Sec 72-A deals with the disclosure of information in breach of lawful contract.

Sec 72A. Punishment for disclosure of information in breach of lawful contract.–Save as otherwise provided in this Act or any other law for the time being in force, any person

[10] Section 43A in the Information Technology Act, 2000,

 [ISSN 2581-5369]

including an intermediary who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person, shall be punished with imprisonment for a term which may extend to three years, or with fine which may extend to five lakh rupees, or with both.[11]

This section prohibits the employer from disclosure of personal information of the employees without the consent of the concerned person.

Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules

The SPDI rules shall be applicable to any person or a body corporate located within the territory of India. These rules require any person or body corporate processing sensitive personal information to comply with certain procedures.

Employer's Obligations

The employers collect various information from the employees including personal information, medical information, financial information etc. Certain responsibilities come into picture on the part of the employers to protect the data and privacy.

SPDI rules requires the employer to initially draft a privacy policy which includes the nature of information collected, the purpose and the reasonable practices adopted by the employer. This privacy policy shall be published on the employer's website and shall be proffered to the employee.[12]

LOOPHOLES IN INDIA'S EMPLOYEE PRIVACY LAW

Evaluating the employee's privacy policy of India, one can witness a number of loopholes. There is no dedicated single and particular legislation to encounter the need and protection of the privacy regime in India. The IT Act, 2000 and SPDI rules provide a legal framework on this subject, but a definite law is missing. The protection and laws prevailing in India is not sufficient to bring the employers under the liability for non-compliance.

Firstly, the term 'data' under the IT Act, 2000 and the SPDI Rules create confusion as they are contradictory to each other in nature. The definition part of the IT Act has to be revamped as it restricts to computer based data. With the advent of fast growing technologies, the restrictive

[11]Section 72A in the Information Technology act, 2000, Indiankanoon, https://indiankanoon.org/doc/69360334/.
[12]Data privacy regime in India: IT Act and SPDI Rules, Preview Tech News (15 August 2018), https://previewtech.net/data-privacy-it-act-spdi-rules/.

 [ISSN 2581-5369]

definitions can easily make the employers escape from liability.

Secondly, there lacks a clear demarcation between the personal data and sensitive personal data.

Thirdly, the laws have inadequate penalties. The monetary effect of the penalties is not sufficient to have a deterrent impact on the body corporate.

Lastly, the level of data protection required for different sets of information is not clearly defined. The act prescribes same level of protection to all the information.

PERSONAL DATA PROTECTION BILL, 2019

The individual's choice gained emphasis as an important branch of privacy after the Supreme court's ruling on 2017. The Personal Data Protection Bill, 2019 was introduced as a marching step towards privacy protection. The bill was introduced on December 11, 2019. This bill was introduced to protect the personal data of the individuals. This bill also touches upon the employee's personal data protection unlike the GDPR. Being a welcoming move towards the privacy protection regime, this bill has still not gained its place in the today's laws.

III. CONCLUSION

Where every countries have taken the GDPR as a model to implement their data protection laws, India has taken one step ahead in introducing the Personal Data Protection Bill, 2019 covering many aspects of privacy in separate heads. One of such is the employer- employee relationship and the data privacy.

To sum up, the authors are of the view that privacy being an indispensable part of everyone's life, it is high time for India to implement and take steps on enacting it as a law. Henceforth, it is advisable that India takes quick steps in implementing the bill into an Act. The EU model can be taken as a reference and steps shall be taken to remove all the drawbacks which the EU model have. A comprehensive legislation on data protection including the employee's privacy in particular has to be enacted.

*****

 [ISSN 2581-5369]