III. EMPLOYER AS DATA FIDUCIARY: A NEGLECTED PROTECTION OR AN EXAMPLE OF POWER IMBALANCE?

- Intisar Aslam and Garima Kiran*

ABSTRACT

The laws of labor have always gained traction- the credit goes to the debates on the long working hours and no work-life balance. This takes the clock backwards to 1817 when Robert Owen formalized the goal of the Eight-Hour Work Day. While this social movement was focused on the rights of workers, the line of variance for employees has been blurred with time. Employment contracts, an 'act of submission' as termed by Kahn-Freund, found their roots in the old master-servant relationship. With the prime object of labor law being to be a countervailing force to the inherent inequality of bargaining power, little did employees know that the perforation of technology in the ever-evolving industrial world would entail the protection of their data collected by these industrial establishments. Though the Indian legislative picture has been painted with the enactment of the Digital Personal Data Protection Act, 2023, the Labour Codes remain unenforced in the territory of India. Notably, the Labour Codes are rather indifferent to the protection of data of any kind. Broadly, this paper has three aims. First, the authors underscore the need for the protection of employee data and the subsequent inadequacy of the present framework to address the same. Second, we explore the employer as a significant data fiduciary while highlighting the challenges of secondment. Next, we argue that employee consent may not be free. Lastly, the authors assess the stance of India in the cross-border transfer of employee data and conclude with a beneficent rule of construction.

* The authors are third-year students of B.A. LL.B. (Hons.) at National University of Study and Research in Law, Ranchi. Views stated in this paper are personal.

I. INTRODUCTION

India has witnessed several data breaches of employees like the HR portal of myrocket.co, Okta, etc.[1] In July 2023, a massive breach of employee data of the largest public sector bank in India, the State Bank of India ("**SBI**"), took place, where the data of more than 12,000 SBI employees was leaked on Telegram.[2] The leaked data of the SBI employees included personal information like names, addresses, contact numbers, PAN details, etc. Such leakages form the *foremost* reason not only for the protection of employee data but also emphasize the positioning of the organization as an accountable and ethical entity in the commercialized world. It is worth mentioning that SBI is an instrumentality of the State.[3] The Digital Personal Data Protection Act, 2023 ("**DPDP Act**") makes a provision for the exemption of the state and/or its instrumentalities from the provisions of the statute on the grounds of sovereignty and integrity of the country, public order, etc. Essentially, the central government can, at any time, free SBI from the clutches of this statute,

[1] The Hindu Bureau, 'HR Portal myrocket.co data breach exposes information of Indian employees: Report' (*The Hindu* 18 January 2023) <https://www.thehindu.com/sci-tech/technology/hr-portal-myrocketco-data-breach-exposes-information-of-indian-employees-report/article66396467.ece> accessed on 10 November 2023; Bill Toulas, 'Okta hit by third-party breach exposing employee information' (*Bleeping Computer* 2 November 2023) <https://www.bleepingcomputer.com/news/security/okta-hit-by-third-party-data-breach-exposing-employee-information/#google_vignette> accessed on 10 November 2023.

[2] Bidisha Saha, '12,000 SBI employees' sensitive date leaked on Telegram channels' (*Business Today* 11 July 2023) <https://www.businesstoday.in/technology/news/story/12000-sbi-employees-sensitive-data-leaked-on-telegram-channels-389239-2023-07-11> accessed on 10 November 2023.

[3] M/s Legal Property & ANR and Chief Manager, State Bank of India & ANR [2023] LiveLaw (Kar) 298.

including the mandatory provision for the protection of data being stored or processed by it.[4] Such exemptions go against the interest of the employees with neither any measure to safeguard such data nor any remedy to pursue in breach of the same.

Secondly, the collection of a voluminous amount of employee data necessitates the need for effective management and protection of data. With a larger volume of data comes greater risk and therefore, regulation and monitoring are essential to minimize the risks of breaches. On these lines, the earlier draft of the Personal Data Protection Bill of 2018 through Clause 16 provided employment as a basis for processing only non-sensitive personal data.[5] Information such as sexual orientation, transgender status, caste, religion, etc. was covered under sensitive personal data. However, in the latest framework, employers have been given a free hand to elicit broad-based consent to process such sensitive information. Thus, there is also a high possibility of rampant discrimination based on caste, gender, and religion in workplaces.

Thirdly, the protection of employee data is crucial in the administration of benefits such as the Employees' Provident Fund ("**EPF**"). There is no use in providing benefits to an employee when, on the other hand, their personal data is being compromised. Eventually, it is a no-win, no-loss situation. Safeguarding employee data would help ensure the accuracy of records and the receiving of benefits to which they are entitled without any error or discrepancy. Furthermore, the benefits of insurance often require the details

[4] Digital Personal Data Protection Act 2023, s 8(5).
[5] Personal Data Protection Bill, 2018, cl 16.

of family members, thereby, further fortifying the need for protection of data by the employer.

Additionally, there are various other employment benefit programmes such as retirement plans that involve financial transactions. Besides the aforementioned, the health information of the employees also needs to be protected to build and preserve trust that their medical records are handled in a responsible manner by the employers. The same is practiced in the United States where the Health Insurance Portability and Accountability Act of 1996 ("**HIPPA**") requires the creation of national standards to protect sensitive personal information from being disclosed without the patient's consent.[6]

Section 42(1) of the Occupational Safety, Health, and Working Conditions Code, 2020 ("**OSHW Code**") read with Sections 70(3), 82(c), 85(a) and (c), 93(5) require medical assessment if the workers to ensure their fitness to perform diverse activities.[7] As per Section 85(1) of the OSHW Code, the occupier of a factory is required to maintain accurate health and medical records.[8] Such provisions including providing an assessment by a registered medical practitioner may give rise to data protection implications for the workers. Thus, employers must determine the legal basis before processing such data to ensure the lawfulness of the same.

In sum, the protection of employee data is integral for maintaining trust, ensuring fair treatment, and upholding ethical practices within

[6] Heath Insurance Portability and Accountability Act 1996.
[7] Occupational Safety, Health, and Working Conditions Code 2020.
[8] Occupational Safety, Health, and Working Conditions Code 2020, s 85(1).

organizations. Neglecting data protection not only jeopardizes individuals' privacy but also undermines the integrity of employee benefits programs.

II. CURRENT LEGAL FRAMEWORK OF INDIA

The earliest legislation on data protection in India has been the Information Technology Act of 2000 ("**IT Act**").[9] The existing literature has relied upon the same to make room for the protection of employee data through the applicability of provisions like Sections 43A, 72, and 72A.[10] However, while making room for its applicability, voids effecting inapplicability have been a go-by.

A. The IT Act Lens: Straightjacket Provisions of Negligent Disclosure

Section 43A imposes liability on body corporates that are negligent in dealing with 'sensitive' personal data.[11] The incorporation of '*negligence'* i.e., failure to exercise a duty of care in terms of tort law, imposes a civil liability on the body corporates. Essentially, the underlying meaning of such a provision revolves around the act and omission of body corporates. If there is a breach of the personal data of an individual, and the body corporates have maintained reasonable security practices and procedures, they shall not have any liability eventually, leaving the individual with no remedy. Section 72 is a saving provision that provides for a penalty for breach of confidentiality and privacy through the disclosure of any information about an individual to a third

[9] Information Technology Act 2000.
[10] Rakhi Jindal, Gowree Gokhale, Vikram Shroff, 'The Indian legal position on employee data protection and employee privacy' (*Nishith Desai Associates*, March 2012) <The_Indian_legal_position_on_employee_data_protection_and_employee_privacy.pdf (nishithdesai.com)> accessed 10 November 2023.
[11] Information Technology Act, 2000, s 43(A).

party without his consent.[12] While this provision gives importance to the consent of the data principal while sharing its data with a third party, it is yet again a provision that makes space for the body corporate or the 'original' data fiduciary to escape liability if it processes the data for its own purpose. Another saving provision, Section 72A, is a slightly different provision where disclosure is in breach of a lawful contract.[13] This provision, therefore, might reflect some resemblance with the employment contracts. At the same time, a scrutiny of the provision reveals that the obligations imposed therein are confined to persons '*providing'* services under the lawful contract. The distinction herein lies between '*providing'* and '*availing'*. Instead of imposing obligations of disclosure on body corporates or intermediaries '*availing'* services from individuals, the provision turns the situation topsy turvy. In sum and substance, the aforementioned provisions of the IT Act fail to bring employee data within its ambit to any extent whatsoever.

B. Data Processing and Third Parties: Liability or No Liability?

In 2011, in the exercise of the powers conferred by Section 43A read with Section 87(2)(ob), the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules ("**SPDI Rules**") was brought in by the government.[14] It is pertinent to note here that the SPDI rules provide for sensitive personal data- a categorization that finds no place in the recent data protection framework of India. While it is anticipated that the IT Act shall be replaced by the Digital India Act, it is important to assess its overriding effect on the DPDP Act for the time being it

[12] Information Technology Act, 2000, s 72.
[13] Information Technology Act, 2000, s 72(A).
[14] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, GSR 313(E).

is in force in light of the categorization of data.[15] Section 81 of the IT Act gives the statute an overriding effect over any law inconsistent with its provisions for the time being in force.[16] The primary contour of the applicability of this provision is the inconsistency between two similarly placed legislations.[17] In the DPDP Act, while there is no provision for the categorization of personal data, there is nothing to indicate that the legislative intent was to proscribe such categorization thereby, giving rise to any inconsistency. In the absence of otherwise, the IT Act could be read harmoniously with the provisions of the DPDP Act to establish a robust framework for India. However, the SPDI rules only address a smaller circle of issues and focus heavily on three aspects*: (i)* Disclosure of data and not processing; *(ii)* Liability for disclosure by body corporates and not third parties; and *(iii)* employee consent and lawful contracts. It is noteworthy that a 'lawful' contract is an exception to waive the obligation of obtaining consent to disclose such personal data. As a conclusion, the IT Act as a whole cannot delve into the purpose of holding data, the manner in which it was obtained, the duration of retention, security and encryption, and grounds for third-party sharing.[18]

[15] Anika Chatterjee, 'India to introduce new Digital India Act to regulate Big Tech' *The Hindu Business Line* (01 May 2023) <https://www.thehindubusinessline.com/info-tech/india-to-introduce-new-digital-india-act-to-regulate-big-tech/article66799883.ece> accessed 10 November 2023.

[16] Information Technology Act 2000, s 81.

[17] *Sharda Devi v. State of Bihar* [2002] 3 SCC 705.

[18] Editor, 'Data Protection in the Workplace' (*Citizens Information Centre*, 03 June 2022) <https://www.citizensinformation.ie/en/employment/employment-rights-and-conditions/data-protection-at-work/data-protection-in-the-workplace/> accessed 10 November 2023.

III. THE DATA PROTECTION FRAMEWORK AND ITS INACCESSIBLE REMEDY TO EMPLOYEES

The question that arises now is whether the new data protection framework brings employee data within its ambit. Before delving into this question, an interesting case of First Choice Selection Services Limited ("**FCSSL**") must be discussed.[19] It is often witnessed that aggrieved employees file cases against their employer but lack information, which is indispensable for their claims to be successful. Consequently, even prior to commencing legal proceedings in the court of law, it is commonplace for employees in foreign jurisdictions to submit a Data Subject Access Request ("**DSAR**") to their employer. This request seeks copies of personal data that employees believe their employer holds. Obtaining such data can notably bolster cases that initially appeared weak.

In the FCSSL case,[20] the employer had wilfully refused to release the information to the employee to pursue its claim against the employer. The Office of the Information Commissioner held that the employer had breached its data protection obligations to the employee. The Indian data protection framework gives the right to the employer to process personal data as a '*legitimate use*' to safeguard itself from loss or liability under Section 7(i) of the DPDP Act.[21] Further, it specifically empowers the employer to process the data of its employee for "*provision of any service or benefit sought by a Data*

[19] Information Commissioner, 'Enforcement Notice' (*Information Commissioner Office* 02 March 2021) <https://ico.org.uk/media/action-weve-taken/enforcement-notices/4017978/first-choice-selection-services-limited-en.pdf> accessed 10 November 2023.
[20] ibid.
[21] Digital Personal Data Protection Act 2023, s 7(i).

Principal who is an employee."[22] Apart from this employer-centric provision, no provision in the DPDP explicitly provides for the right to data protection of employees in the same manner as the employer has for processing. While social welfare legislations are being implemented, the inherent imbalance of power manifests itself in other forms and characters. Moreover, this gap in power is widened by the absence of a provision for Data Subject Access Request which would facilitate the pursuit of remedies by the employee for potential data breaches by the employer. Though Section 11 of the DPDP Act provides for access to personal data, this provision can be relaxed for the State and its instrumentalities under the exemptions provision.[23] It is unclear, therefore, if an employee would be able to seek a remedy against a state or its instrumentality in case of any grievance. The situation is akin to a locked door without a key: the remedy lies beyond but remains inaccessible. Though the legislation has been armed with the phrase 'data protection', in the labour jurisprudence, the provisions contained therein outcry an employer-centric processing framework.

IV. EMPLOYEE FAVORITISM: PROTECTION OF EMPLOYEE DATA OR DIGITAL EMPLOYEE DATA?

The Digital Personal Data Protection Act, 2023 gives a broad definition of a Data Principal to include any individual to whom the personal data relates.[24] Along similar lines, a data fiduciary includes any person who determines the purpose and means of processing personal data while a data

[22] ibid.
[23] Digital Personal Data Protection Act 2023, s 11.
[24] Digital Personal Data Protection Act 2023, s 2(j).

processor processes such data.[25] Section 2(s) gives clarity to these provisions, which define a person not only as an individual but also as a firm, company, or association of individuals, etc.[26] Clearly, an employer and an employee can fall under the respective ambits of data fiduciary and data principal but only in respect of digital data and not offline data. Thus, any employee data collected through offline means or data pertaining to labourers would fall outside the ambit of the DPDP Act. Furthermore, two questions that arise are: *(i)* Given that the employers collect voluminous, sensitive data about the employees, whether they all be notified as significant data fiduciaries? and *(ii)* In cases of secondment of employees, who shall be the data fiduciary and/or data processor?

A. Employers as Significant Data Fiduciaries

Section 10 of the DPDP Act determines a few factors to assess any data fiduciary as significant data fiduciary.[27] These include the volume and sensitivity of personal data processed, the risk to the rights of Data Principals and electoral democracy, and the potential impact on the sovereignty, integrity, security of India, and public order. With regards to the sensitivity of personal data, it is evident that employers not only collect data related to sexual orientation, physical and physiological conditions but also biometric and financial information of the employee.[28] In a recent case, the Dutch Data Protection Authority observed that the processing of biometric data was not

[25] Digital Personal Data Protection Act 2023, s 2(i); Digital Personal Data Protection Act 2023, s 2(k).
[26] Digital Personal Data Protection Act 2023, s 2(s).
[27] Digital Personal Data Protection Act 2023, s 10.
[28] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, rule 3.

necessary for authentication or security purposes under the General Data Protection Regulation ("**GDPR**").[29] When it comes to the volume of data collected, employers also collect salary data, surveillance through security cameras, business trips, personal messages on company phones, and location data of the company car for private trips.[30] The list is not exhaustive and makes it evident that an employer can *prima facie* fall within the bracket of significant data fiduciaries. However, the usage of the term '*may*' gives discretion to the central government to impose any additional obligations on the employer. In *arguendo*, Section 17(3) gives the central government to exempt any government or private entity from these additional obligations, including obligations to protect personal data, serve notice to data principals, erasure of data post fulfilment of purpose, and provide access to information about personal data.[31] This brings India back to square one- the imbalance of power between an employer and employee- shifting the balance again in favour of the employer.

B. Secondment of Employees: Who is the Data Fiduciary and who is the Data Processor?

Article 4(16) of the GDPR defines the main establishment of a data fiduciary and data processor respectively in situations where there is more than one establishment.[32] For these purposes, the main establishment is where the

[29] Debbie Heywood, 'Processing Employee Fingerprint Data' (*Taylor Wessing*, 10 July 2020) <https://www.taylorwessing.com/en/global-data-hub/2020/july---hr-data/processing-employee-fingerprint-data> accessed 10 November 2023.
[30] Barnea Jaffa Lande & Co, 'Collecting Employee Information? It's Time to Wake Up' (*JD Supra*, 12 January 2021) <https://www.jdsupra.com/legalnews/collecting-employee-information-it-s-6974458/> accessed 10 November 2023.
[31] Digital Personal Data Protection Act 2023, s 17(3).
[32] General Data Protection Regulation (EU) 2016/679.

central administration takes place, unless some other establishment has the power to make decisions related to the purposes and means of processing personal data. Furthermore, in the recent case of *Yung Wai Tak Abraham William* v. *Natural Dairy (NZ) Holdings Ltd.*, the Court of First Instance held that a company could be the employer of the seconded employee even though there is no written employment contract between them.[33] In this case, the employee had no knowledge of his secondment, and no agreement was entered into to effect secondment. Moreover, since employees mainly had to deal with the work of the parent company, it constituted a separate employer-employee relationship despite the existence of an employment contract with the subsidiary company. This judgment is on similar lines with the Indian rulings laying importance on the language of the secondment agreement and, in its absence, the company having a greater degree of control, supervision, responsibility, termination, remuneration, etc.[34]

The DPDP Act, on the other hand, does not give any such reference to the place of establishment of a data fiduciary or processor and therefore, poses challenges in processing personal data in situations like secondment. It is the temporary transfer of an employee, whether domestic or international, for a short period within a company in the same organization or between different entities.[35] While secondments typically happen through agreements, in a

[33] [2020] HKCFI 2067.

[34] *Centrica India Offshore Pvtl Ltd v. Income Tax-Ia* [2014] SCC OnLine Del 2739; *DIT (International Taxation) v Abbey Business Services India (P) Ltd* [2020] 122 taxmann.com 174 (Kar).

[35] Editor, 'Glossary: Secondment' (*Practical Law*) <https://uk.practicallaw.thomsonreuters.com/1-521-1558?transitionType=Default&contextData=(sc.Default)&firstPage=true#:~:text=The%20temporary%20assignment%20of%20an,between%20two%20unrelated%20business%20entities> accessed 10 November 2023.

situation otherwise, the lines between the data fiduciary and the data processor would be blurred. Even if the same are clearly identifiable, the likelihood that the consent of the employee would be '*presumed*' to have been given in respect of another entity is unsettling.

C. Cross-border Employee Data Transfer: Where does India stand?

Due to globalization, companies strive to have a global presence and to spread their operation in different jurisdictions, transfer of employee data beyond the national borders is necessary. In the European Union, GDPR allows for the transfer of data to a foreign jurisdiction or third party while ensuring the adequate and equivalent level of protection and safeguards as provided in the jurisdictions where the data is being transferred.[36] Furthermore, cross-border data transfer requires that the standard of protection offered by the data controllers and processors transmitting such data must be "*essentially equivalent*" to that offered by the General Data Protection Regulation.[37]

Similarly, in jurisdictions like Brazil and Singapore, the laws require that the jurisdiction to which the data is transferred must provide an adequate level of protection and employ necessary safeguards to protect the transferred data.[38] Along the same lines, the New Zealand Privacy Act 2020 also requires due diligence to be exercised over the third party to whom the data is being

[36] Editor, 'HR Data Security: HR's Role in Employee Privacy & Data Protection' (*KBI*, 5 January 2023) <HR Data Security and Employee Privacy | KBI Benefits> accessed 10 November 2023.
[37] *Data Protection Commissioner v Facebook Ireland* [2020] C-311/18.
[38] Securiti Research Team, 'The HR Guide to Employee Data Protection' (*Securiti*, 11 August 2023) <The HR Guide to Employee Data Protection - Securiti> accessed 10 November 2023.

transferred to ensure compliance with the Act.[39] Thus, in essence, the stand of most jurisdictions is similar allowing transfer on grounds of the essentially equivalent principle.

On the other hand, the DPDP Act has undergone a series of transformations over time. The earlier drafts had come up with a local storage obligation for sensitive personal data and a hard localization obligation for an undefined category of critical personal data.[40] Next, the Digital Personal Data Protection Bill, 2021 envisioned whitelisted countries where cross-border transfer was permitted.[41] This provision is similar to the laws of foreign jurisdictions. However, in the latest 2023 framework, through Section 16, the legislature has taken a negative approach conferring the power on the Central government to notify certain blacklisted countries where the data transfer shall not be allowed.[42] At the same time, sub-section 2 also provides that the Act would not render any other existing law ineffective that imposes a higher degree of protection or restrictions on personal data transfers but it remains silent on the standard of protection that should be provided when the data is transferred overseas.[43] Further, the silence of the Act extends to the duty that the employers have during the transfer of cross-border employee data.

A 2019 report emphasized that realizing India as a $1 trillion digital economy hinges on establishing a conducive environment where capital, innovation, data, and design capabilities can seamlessly move to nations that

[39] Dr Sam De Silva & Elizabeth Vincent, 'New Zealand- Data Protection Review' (*One Trust Data Guidance* October 2022) <https://www.dataguidance.com/notes/new-zealand-data-protection-overview> accessed 10 November, 2022.
[40] Personal Data Protection Bill 2018, s 40.
[41] Digital Personal Data Protection Bill 2022, s 17.
[42] Digital Personal Data Protection Act 2023, s 16(1).
[43] Digital Personal Data Protection Act 2023, s 16(2).

present fewer obstacles.[44] However, while making India '*digital*', any digital trade-off or, to put it differently, putting the employee data at stake would defeat the purpose of the vision *per se*. It is therefore important to strike a balance between flourishing global markets through seamless transfer and the basic rights and interests of the employees.

V. *BRAHMASTRA* OF THE EMPLOYER: IS THE EMPLOYEE CONSENT RELIABLE?

In an employer-employee relationship, the power imbalance between the two is a very common feature. The imbalance between the two is the outcome of several factors like access to financial resources, decision-making authority, and employment contracts whose terms and conditions are often determined by the employers. All these factors contribute to creating an imbalance of power between the two where the employer is at a higher pedestal than employees. Sir Otto Kahn-Freund, one of the greatest jurists of the twentieth century and scholar of labor law, viewed the relationship between the employer and an employee as a relationship between the bearer of power and one who is not a bearer of power.[45] It means an act of subordination where the employee submits to the employer. He believed such subordination to be inherent in any employment relationship and it could not be replaced by coordination between the two.

---

[44] Ministry of Electronics and Information Technology, 'India's Trillion-Dollar Digital Opportunity'
(2019) <https://web.archive.org/web/20220604181319/https://www.meity.gov.in/writereaddata/files/india_trillion-dollar_digital_opportunity.pdf> accessed 10 November 2023.

[45] Paul Davies and Mark Freedland, *Kahn-Freund's Labour and the Law* (3rd edn Stevens 1983) 18.

Even at present, there persists a fundamental imbalance in the bargaining power of employers and employees. As long as the employers have the authority to hire and fire making the employees vulnerable to sudden terminations, they set the terms and conditions of employment providing the employees with limited negotiation power. There are serious repercussions that prevail due to inequality in power like the lack of freedom for employees in the workplace, a threat to employee rights and protection, income inequality, and systemic race and gender discrimination.[46]

While such an imbalance persists, the consent given by the employees for processing their personal information by the employers cannot be regarded as free. The significant imbalance of power could lead an employee to act under a mental compulsion to comply with the employer's requests for consent. It is beyond doubt that the fear of getting fired from the post and/or other adverse consequences has the potential to undermine the voluntariness of the consent.

This imbalance can very much be demonstrated by two contemporary instances: *First*, the data privacy notice of Microsoft which disbelieves in obtaining the consent of its employees for processing most of their data unless it is legally required.

The privacy policy of Microsoft lays down,

"*The unique nature of the employment relationship means that choice may be more limited or not available for certain kinds of data processing (payroll processing for example). Similarly, where Microsoft*

[46] Worker Stories, 'Unequal Power' (*Economic Policy Institute*) <https://www.epi.org/unequalpower/home/> accessed 10 November 2023.

has legal or contractual rights or obligations to process or disclose data, we cannot allow for choice in how that data is used."[47]

Furthermore, Microsoft claims to offer its employees the choice as to how the data may be processed but only when '*it'* believes it appropriate. Additionally, owing to the nature of the relationship and the subsequent subordination, the choices given to the employees are very limited and are not available for all kinds of data processing.

Second, in a case decided by the Dutch Data Protection Authority, the decision was delivered in favor of the employee which was based upon an observation that in instances where an employee had initially refused consent, the employee had ended up agreeing to provide their fingerprints after the interview with the director.[48]

While the DPDP Act requires that the consent given by the Data Principals should be free for processing personal data[49], labour laws would play a major role in diminishing the imbalance of power between employers and employees by establishing a framework that ensures fairness and a balanced employment relationship. The Industrial Relations Code, 2020 ("**IR Code**") for instance, provides for penalties to be imposed on employers, workers, and trade unions for committing any unfair labour practices under Section 84.[50] The second schedule of the IR Code provides for all such acts

[47] Microsoft, 'Microsoft Global Data Privacy Notice for Employees, External Staff, Candidates and Guests' (October 2023) <https://privacy.microsoft.com/en-us/data-privacy-notice> accessed 10 November 2023.
[48] Debbie Heywood, 'Processing Employee Fingerprint Data' (*Taylor Wessing*, 10 July 2020) <https://www.taylorwessing.com/en/global-data-hub/2020/july---hr-data/processing-employee-fingerprint-data> accessed 10 November 2023.
[49] Digital Personal Data Protection Act 2023, s 6.
[50] The Industrial Relations Code 2020, s 84.

that constitute unfair labour practices which include interference with the rights of the workers to engage in collective bargaining by threatening workers with their dismissal or discharge.[51] Therefore, in the absence of any specific provision both in the DPDP Act and the Labour Codes, a harmonious application of both laws shall go a long way in ensuring the protection of employee data until interpretative rules are framed in this regard.

VI. CONCLUSION

Article 88(1) of the GDPR makes specific provisions for the protection of employee data by law and by collective agreements. It provides,

"Member States may, by law or by collective agreements, provide for more specific rules to ensure the protection of the rights and freedoms in respect of the processing of employees' personal data in the employment context, in particular for the purposes of the recruitment, the performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organisation of work, equality and diversity in the workplace, health and safety at work, protection of employer's or customer's property and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship."[52]

On the contrary, the Labour Codes or the DPDP Act do not provide for any explicit provision in the interest of the employee. Therefore, at *first*, for the purposes of labour jurisprudence, the DPDP Act must be construed as

[51] The Industrial Relations Code 2020, Second Schedule.
[52] General Data Protection Regulation (EU) 2016/679.

social welfare legislation. According to the rules of interpretation, the beneficent rule of construction of the provisions must be carried out to include employees, wherever possible.[53] At present, the only ray of hope provided by the lawmakers is the framing of broadly worded provisions of the legislation.

Secondly, pursuant to Section 40(1),[54] it is necessary for the Central government to frame rules under this Act to facilitate its proper implementation and provide further clarity on the provisions. Since secondment may also involve the assignment of employees to foreign entities, the rules may include provisions outlining factors based on which a distinction could be made between a data fiduciary and a data processor not only in cases of secondment but also for the cross-border sharing of data.

Thirdly, offline data collected by employers must be brought into the ambit of the statute. The DPDP Act leaves a large chunk of the working population in the lurch for the protection of their personal data. The labour force participation rate in India increased to 42.4% in Dec 2023, compared with 41.3% in the previous year.[55] In the 2011 Census[56], it was revealed that 21.9 million marginal workers consisted of individuals lacking literacy. This

---

[53] *Workmen v. Firestone Tyre & Rubber Co of India (P) Ltd* [1973] 1 SCC 813.

[54] Digital Personal Data Protection Act 2023, s 40(1).

[55] CEIC, 'India Labour Force Participation Rate' <https://www.ceicdata.com/en/indicator/india/labour-force-participationrate#:~:text=India%20Labour%20Force%20Participation%20Rate%20increased%20to%2042.4%20%25%20in%20Dec,an%20average%20rate%20of%2054.2%20%25%20> accessed 10 November 2023.

[56] Prashant K. Nanda, 'Most Indian Workers are either illiterate or poorly educated, says Census Data' *Mint* (06 November 2015) <https://www.livemint.com/Politics/NlwY9eAAfRqkKE2vR2AeAP/Most-Indian-workers-are-either-illiterates-or-poorly-educate.html#:~:text=%E2%80%9CCensus%202011%20has%20shown%20that,Census%20Commissioner%20of%20India%20underlined> accessed 10 November 2023.

was trailed closely by 20.9 million individuals accounting for 37.6% who had received education below the secondary level.

Conclusively, the paper outlines several instances where the amount of control the employers exercise over the employees' data is unrestricted and unbridled. However, such regulation cannot be unreasonably intrusive. In a country like India, where employment generation is a serious concern, data protection of employees holds immense significance for buttressing the broader economic landscape. The trust built in employees about the protection of their personal data would eventually encourage their active participation in the Indian economy.