# [IN] ADEQUACY OF THE DPDP ACT VIS-À-VIS RIGHT TO PRIVACY AT WORKPLACE

Harshita Gupta
*IV Year Law Student, National Law University Jodhpur [B.A.LLB (IPR Hons.), Email: harshita.gupta@nlujodhpur.ac.in*

Dhaani Bharat Dave
*IV Year Law Student, National Law University Jodhpur [B.A.LLB (IPR Hons.), Email: dhaanibharat.dave@nlujodhpur.ac.in*

**Abstract**

*The world is witnessing a digital revolution. Algorithms are steadily sneaking into all aspects of our lives influencing our day to day affairs. The steady increase in datafication of the small mundane realities of life makes one fear about the rise of surveillance not only by the state but private entities as well. In India, though the Puttaswamy Judgment recognised the right to privacy particularly informational privacy as part of Article 21, the enforcement of the Digital Personal Data Protection Act ["DPDP Act" or "the Act"] is still awaited. The DPDP Act, as per its Preamble tries to strike a balance between the right to privacy and the right to process data. However, the Act does not define 'privacy'. This raises the suspicion- whether the act is adequately equipped to protect privacy? India's privacy framework will be applicable on myriad sectors such as healthcare, digital governance, compliance by corporate houses et cetera. This paper is an attempt to investigate into the aspect of how far the DPDP secures the right to privacy especially informational privacy at workplace. This investigation is significant not only in the background of rise in the use of monitoring tools but also because of skewed employee-employer power dynamic. This paper tries to understand the potency of the Indian data protection law in the background of employee privacy by firstly understanding various provisions that affect privacy at workplace in general and thereafter shift the focus to Section 7(i) of the Act. We delve into the history of the provision in this regard and do a comparative analysis with the similarly placed provision in the General Data Protection Regulation and Personal Data Protection Act, Singapore. Thereafter, we shall offer some suggestions on how data privacy can be better protected at workplace by making suitable amendments to the certain provisions in the Act and thereafter provide a conclusion.*

**Keywords:** Digital Personal Data Protection Act, employee's privacy, informational privacy, legitimate interest, employment purpose, workplace surveillance.

## 1. Introduction

Technology has opened doors to better standards of living however it has also facilitated the entry of unwanted gaze over our lives. There exist multiple tools to surveillance people in general as they go about their lives.[1] The same is true for persons under any form of employment are at the risk of constant monitoring by their employers through various tools

[1] Luciano Floridi, *On human dignity as a foundation for the Right to Privacy*, 29 PHILOS. TECHNOL., 4 (2017) https://dx.doi.org/10.2139/ssrn.3839298.

such as *Bossware* and *Workpuls*.[2] Such kind of software gives unbridled access to the data such as browsing history, emails to the employers. The collection of biometric data is also quite common at workplace.[3] Though in such cases, the employees are aware of the data being taken, there are two important concerns. Firstly, about the legitimacy of consent of the employees given that the employers always have an upper hand over the employee due to the power asymmetry and secondly, about the risk of data breach.[4] The latter concern is exacerbated by a number of instances of data breaches.[5]

In a number of studies carried out, it has been revealed the surveillance at workplace is becoming pervasive.[6] The technologies are making it possible for employer to not only track efficiency but also movement, behavior et cetera. The use of this kind of monitoring is more rampant in work from home settings.[7] Concerns have also been raised about the future of privacy at workplace in light of various emerging technologies and their capability to monitor employees engaged in a variety of activities sometimes also blurring the lines between personal and professional information.[8] In India too it has been reported by various organisations that workplace surveillance is gaining traction.[9] Concerns have also been raised about privacy of

[2] Jeevan Hariharan & Hadassa Noorda, *Imprisoned at Work: The Impact of Employee Monitoring on Physical Privacy and Individual Liberty*, 88(2) MOD. L. REV., 333, 333-365 (2024); Henry Parkes, *Watching me, watching you: Worker surveillance in the UK after the pandemic*, IPPR (Mar. 2023), https://ippr-org.files.svdcdn.com/production/Downloads/worker-surveillance-mar23.pdf ;
Aiha Nguyen, *The Constant Boss: Work under Digital Surveillance*, DATA & SOCIETY (May 2021), https://datasociety.net/wp-content/uploads/2021/05/The_Constant_Boss.pdf ; Zoe Corbyn *'Bossware is coming for almost every worker': The software you might not realize is watching you,* THE GUARDIAN (Apr. 27, 2022, 09:30 AM) https://www.theguardian.com/technology/2022/apr/27/remote-work-software-home-surveillance-computer-monitoring-pandemic ; Julia Gray, *The Bossware Boom is upon us: A look inside the employee monitoring software Market,* THE BUSINESS TO BUSINESS (Oct. 2, 2021, 6:30PM) https://www.businessofbusiness.com/articles/employee-monitoring-softwareproductivity-activtrak-hubstaff-covid.

[3] Kirstie Ball, *Electronic Monitoring and Surveillance in the Workplace*, PUBLICATION OFFICE OF THE EUROPEAN UNION 23 (2021), https://publications.jrc.ec.europa.eu/repository/handle/JRC125716

[4] Guidelines 05/2020 on consent under Regulation 2016/679, European Data Protection Board, Cl.21 May 4, 2020, https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf.

[5] Mardav Jain, *The Aadhaar Card: Cybersecurity Issues with India's Biometric Experiment*, THE HENRY M. JACKSON SCHOOL OF INTERNATIONAL STUDIES (Jan. 24, 2025, 9:30 PM) https://jsis.washington.edu/news/the-aadhaar-card-cybersecurity-issues-with-indias-biometric-experiment/

[6] Jeevan Hariharan & Hadassa Noorda, *Imprisoned at Work: The Impact of Employee Monitoring on Physical Privacy and Individual Liberty*, 88(2) Mod. L. Rev., 333, 333-365 (2024).

[7] *Id*.

[8] Devasheesh P. Bhave, Laurel H. Teo, & Reeshad S. Dalal, *Privacy at Work: A Review and a Research Agenda for a Contested Terrain*, 46(1) JOURNAL OF MANAGEMENT, 127-164 https://doi.org/10.1177/0149206319878254

[9] Shweta Mohandas & Deepika Nandagudi Srinivasa, *The Boss will see you now – the growth of workplace surveillance in India, Is Data Protection legislation the answer?,* THE CENTRE FOR INTERNET & SOCIETY (JAN.24, 2025, 10:30 PM) https://cisindia.org/internet-governance/blog/the-boss-will-see-you-now-the-growth-of.;
Deeksha Malik and Shreya Sukhtankar, *Employee surveillance and data privacy: peeping into the legal considerations,* THE ECONOMIC TIMES (Jan. 25, 2025, 6:00 AM) https://hr.economictimes.indiatimes.com/news/workplace-4-0/employee-surveillance-and-data-privacy-peeping-into-the-legal-considerations/114651181.

those engaged in platform work especially when Indian labour law framework does not cover platform work.[10]

Given that privacy is not an abstract concept rather it is the very basis of all the rights which individuals are endowed with, securing informational privacy at workplace therefore becomes a major concern for all of us.[11] Privacy has been recognized by the Indian Supreme Court as an intrinsic part of Article 21 of the Constitution.[12] As per the judgment privacy is integral to human dignity and autonomy. It covers vital aspects of our life such disclosure or non-disclosure of personal information and freedom of choice. Since privacy is a fundamental right, the state has a constitutional duty to protect it. The State is thus under a positive and a negative obligation to protect people from monitoring at workplace. The positive obligation has to be discharged by the state by not taking any step which impinges on privacy and the negative obligation is to prevent other actors to do the same. 13 While, in pursuance of the first obligation the State can enact laws, for the latter obligation the State has to ensure that non-state actors do not infringe upon this right.

The government has enacted the DPDP fulfilling its positive obligation however; it needs to be examined whether the Act in the context of employment adequately protects individuals from infringement of their right to privacy.

This paper including the introduction shall consist of five parts. In the introduction, the authors will try to bring to fore the concerns related to privacy amidst the increasing use of digital tools to surveil employees. Part II we shall firstly understand various provisions that affect privacy at workplace in general and thereafter discuss Section 7(i) of the Act along with discussing the brief history of the provision relating to collection of employees data shall be discussed. In Part III, a comparative analysis with the similarly placed provisions General Data Protection Regulation (hereinafter 'GDPR') and Personal Data Protection Act of Singapore (hereinafter

[10] Ankit Kapoor and Karthik Rai, *Gig economy: a tale of algorithmic control and privacy invasion*, NLSIR ONLINE (Mar. 23, 2023), https://www.nlsir.com/post/gig-economy-a-tale-of-algorithmic-control-and-privacy-invasion; Shobhit S., *India's data protection law: undermininig labour rights in the gig economy,* INDIAN JOURNAL OF LAW AND TECHNOLOGY (Sept. 21, 2024) https://www.ijlt.in/post/india-s-data-protection-law-undermining-labour-rights-in-the-digital-economy ; Dev Mittal and Amritansh Sharma, *Need for legislative action to protect India's gig workers*, BAR AND BENCH, Oct. 29, 2024, 7:37 PM) https://www.barandbench.com/columns/need-for-legislative-action-to-protect-indias-gig-workers

[11] K.S Puttaswamy v. Union of India, (2019) 1 SCC 1, ¶81.

[12] Justice K.S. Puttaswamy (Retd.) & Another. v. Union of India and Others, AIR 2017 SC 4161.

[13] *Id*.

'PDP Act') shall be made.[14] Through Part IV of the article we shall try provide suggestions and Part V will provide a conclusion for the article.

## 2. The DPDP Act and Privacy at Workplace

This part of the paper shall firstly through Part A, study the broader framework of the Act to understand how it affects privacy at workplace and thereafter in Part B try to delve deeper into Section 7(i) of the Act which deals with processing in the context of employment.

### A. Examining India's Data Protection Framework in the Context of Employment

The DPDP Act allows for the processing of data by the data fiduciary in following cases: firstly, consent-based processing, secondly, legitimate use-based processing and thirdly, through exemptions for processing (when the data is processed invoking the second and third ground, consent of the data principal is not required).[15] As mentioned earlier, a unique relationship exists between the employer and the employee, collecting data through consent becomes onerous for the employer.[16] It also becomes a futile exercise because of the power asymmetry between the employer and employee and in most cases, the employee's consent cannot be said to be free consent.[17]

Thus, the DPDP Act, to process employees' data takes the route of using legitimate use as a ground for processing.[18] The relevant section in the Act calls for processing under "*employment purpose*" or "those related to safeguarding the employer from loss or liability, such as prevention of corporate espionage, maintenance of confidentiality of trade secrets, intellectual property, classified information or provision of any service or benefit sought by a Data Principal who is an employee." While the latter part of the section suggests that data processing should be done when it secures the vital interest of the employer or when the employee himself/herself seeks some benefit, the former part of "employment purpose" remains undefined in the Act.[19] The absence of any guidance on the connotation of this term makes the provision prone to misuse.

[14] Regulation (EU) 2016/ 679 of the European Parliament and of the Council of 27 April 2016; The Personal Data Protection Act, 2012, No. 12, Acts of Parliament, 2012 (Singapore).
[15] The Digital Personal Data Protection Act, 2023, § 4(1)(a), § 7(2), § 17, No. 22, Acts of Parliament, 2023 (India).
[16] BN Srikrishna Committee Report, A Free and Fair Digital Economy: Protecting Privacy and Empowering Indians, 116 (2014).
[17] *id.*
[18] *Supra* note 15, § 7(i).
[19] *Id.*

However, before we delve into the issue of "employment purpose" in sub-part B of this section, it would be pertinent to understand other issues in the Act from the perspective of processing employees' data.

Section 5(1)(i) of the Act mandates that before a data fiduciary processes the data under Section 6, he/she has to give notice to the data principal stating the data being collected and the purpose of such collection.[20] Such data collection and purpose specification requirement is thus not applicable to the processing of data of a person at the workplace. Furthermore, as per Section 11 (1) and 12(1), only those data fiduciaries who's consent has been obtained either as per Section 4(1)(a) or 7(a) would be entitled to know what data has been collected, with whom (other data fiduciaries and processors) the data is being shared and can request the correction of the data.[21] Additionally, Section 8(7) states that data of an employee can be retained till the time it is assumed by the employer to be reasonable.[22] This is unlike the case of other data principals who have given consent and can withdraw it or request the erasure of data. The aforementioned provisions thus do not follow the well recognised privacy principals of collection limitation, data quality, and purpose specification and use limitation.[23] It is noteworthy that the B.N. Srikrishna Committee Report focused on data minimization, consent, storage limitation and purpose specification and the same was reflected in the 2018 and 2019 Draft Bills.[24] The Puttaswamy Judgment too focused on these aspects, drawing from other jurisdictions especially the General Data Protection Regulation (hereinafter 'GDPR').[25] However, these principles are unfortunately missing from the Act.

Another important aspect that the Act does not deal with is the use of automated decision making. Though the act describes what it means by automated decision making, it does not regulate it to the extent that it allows processing and decision making with regard to any benefit, scheme et cetera solely on its basis.[26] This is in stark contrast to other legislations like the UK, EU, and Kenya wherein this has been regulated.[27] This regulation is much needed in light of

[20] *Supra* note 15, §5, §6.
[21] *Id*., § 11(1), § 12(1), § 4(1)(a), § 7(a).
[22] *Id*., §8(7).
[23] OCED Privacy Principals, APEC Principals, Convention 108+.
[24] BN Srikrishna Committee Report, A Free and Fair Digital Economy: Protecting Privacy and Empowering Indians, 116 (2014). Data Protection Bill 2018, Data Protection Bill, 2019, Bill No. 373 of 2019 (India).
[25] Justice K.S. Puttaswamy and Another v. Union of India, 10 SCC 1 2017; Regulation (EU) 2016/679 {hereinafter "EU GDPR"}.
[26] The DPDP Act, *supra* note 15, § 2(b).
[27] EU GDPR, Art. 22; UK GDPR, Art. 22(1); The Data Protection Act, 2019, § 35 (Kenya).

the concerns raised by scholars regarding algorithmic control, bias and the opaque nature of such systems, especially concerning people engaged in platform work.[28]

Another crucial aspect that the Act does not address is the question of who is an employee or employer. This is significant because a large amount of data is processed not only of those people who are working in strict sense but also those who may have applied for jobs, interns, persons who may have left one establishment for another, persons on probation, various applicants for a competitive exam for government service and platform workers. All such people in the absence of a definition are at risk of not being covered under the data protection legislation.

The Act unlike its other counterparts across nations does not provide for additional safeguards for collection and processing of 'sensitive personal data' which in some countries is referred to as 'special data'. Such kind of data as the name suggests pertains to individual's sensitive information such as race, ethnicity, sexual orientation, genetic data, biometric data and health data. Other jurisdictions such as the European Union have restricted the processing of such data. The processing is allowed only if additional safeguards have been provided.[29]

**B. Tracing the roots of Section 7(i) of the DPDP Act**

While the DPDP Act is soon going to be enforced, it is crucial to understand how and why the present provision stands so. The precursor to the legislative framework on data protection law in India was the Report drafted by the Committee headed by Justice B.N. Srikrishna.30 The report discussed various aspects of the data protection law along with global practices and suggestion for future draft of the Act. The present Act has been passed by the Parliament after three drafts/bills of the Act were rejected. At the same time a Joint Parliamentary Committee was formed to discuss the second draft of the bill.

This part shall firstly discuss the recommendation of the B N Srikrishna Committee (hereinafter 'the committee') and thereafter discuss the various changes introduced in the consecutive drafts

[28] Kavya Bharadkar, Kaveri Medappa, Mohan Mani, Pradyumna Taduri, & Sachin Tiwari, *Is Platform Work Decent Work? A case of Food Delivery workers in Karnataka*, 10 CENTRE FOR LABOUR STUDIES 9 (2020), https://www.nls.ac.in/wp-content/uploads/2021/09/OCCASIONAL-PAPER-SERIES-10-final.pdf; HENRY, *supra* note 2 ; SHOBHIT, *supra* note 10 ; ANKIT & KARTHIK, *supra* note 10.
[29] EU GDPR, Art. 4(13), 14, 15, 9, Recital no. 51, 56.
[30] BN Srikrishna Committee Report, A Free and Fair Digital Economy: Protecting Privacy and Empowering Indians, 116 (2014).

of the provision on collection of data related to employment along with the Joint Parliamentary Committee's (hereinafter 'JPC Report') analysis of the 2019 Bill.[31]

The Committee recognized that collection of employer's data is required for the employers. Pursuant to the same it suggested inclusion of some situations for non-consensual collection of data. It also recommended collection of data for "*any other activity relating to the assessment of the performance of the employee*". However, this ground was qualified by demonstration of the fact that the consensual collection of such is extremely burdensome for the employer or due to the unique relationship between the employer and employee taking consent becomes a futile exercise.[32]

Section 16 of the 2018 Draft Bill delineated certain situations in which non-consent based data could be taken however this was qualified by two things.[33] Firstly, the use of the term 'necessary' in sub-section (1) and sub-section (2) that allows such collection in extremely onerous situations or where seeking consent involves disproportionate effort on the part of the employer. In the 2019 Draft Bill, Section 13 began with a non-obstante clause which states that this section shall not be subjected to the limitations under Section 11 of the Bill. But sub-section 13 (2) retains the qualification which was incorporated in section 16 of the 2018 draft bill.[34] In the 2022 Draft of the Bill, the concept of 'Deemed Consent' was used.[35] This would mean that under some circumstances, it would be assumed that the consent requirement has been met. Section 8 (7) of the 2022 Bill enlists various situations wherein data can be collect sans consent. However, these situations are non-exhaustive and the sub-section uses the term 'including'. It is pertinent to note here that this Section uses the word 'necessary' with regard to the collection of data. This means that non-consensual processing data is contingent on the necessity of the situation. If the situation does not warrant the same then such collection would not be permitted.

[31] Joint Parliamentary Committee on the Personal Data Protection Bill, Report of the Joint Committee on the Personal Data Protection Bill, 2019, (Lok Sabha Secretariat, 17th Lok Sabha, December, 2021) https://eparlib.nic.in/bitstream/123456789/835465/1/17_Joint_Committee_on_the_Personal_Data_Protection_Bill_2019_1.pdf.

[32] BN Srikrishna Committee Report, A Free and Fair Digital Economy: Protecting Privacy and Empowering Indians, 116 (2014).

[33] Draft Personal Data Protection Bill, 2018, http://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill%2C2018_0.pdf

[34] Draft Data Privacy and Protection Bill, 2019, Bill no. 341 of 2019, https://sansad.in/getFile/BillsTexts/LSBillTexts/Asintroduced/341%20of%202019As%20Int....pdf?source=legislation

[35] Draft Digital Personal Data Protection Bill, 2022, https://prsindia.org/billtrack/draft-the-digital-personal-data-protection-bill-2022.

In the latest 2023 Act, Section 7(i) deals with collection of data of the employers. Unlike the previous drafts wherein data collection was qualified through the use of the terms 'necessary' and 'disproportionate effort' this sub-section gives the employer a free hand. This issue is further exacerbated by the vagueness of the term *'employment purposes'* in sub-section 7(i).

Thus, we note that the Act lacks on several counts along with the nebulous wording of Section 7(i) and does not provide adequate protection from privacy harms at the workplace. This is in striking contrast to other jurisdictions such as the European Union and Singapore which have extensive provisions securing the right to informational privacy at workplace to a great extent.

**3. Comparative analysis of the DPDP act with GDPR and PDP Act**

The DPDP Act being India's First data privacy legislation has taken inspiration from the GDPR and Singapore Data Privacy legislation which is the PDP Act.[36] The DPDP Act, GDPR and PDP Act stand as three of the most extensive data protection legislations globally.

The rationale for comparing these three legislations is that the term *'certain legitimate uses'* has been used under section 2(d) of DPDP Act, Section 4(1)(b) of DPDP Act recognizes '*certain legitimate uses'* as a lawful ground which is an exception to consent. Similarly, EU's GDPR and Singapore's PDP Act have used the term *'legitimate interest'* as a ground for data to be collected without seeking the consent of the data fiduciary. Hence, it is important to look into how European Union's GDPR and Singapore Data Privacy legislation PDP Act has interpreted the term *'legitimate interest'* in the context of the employer and employee relationship.

**A. Comparison between DPDP Act with the GDPR in the context of "Certain Legitimate Use" v. "Legitimate Interest"**

Under the DPDP Act, the employer can access the data of the employee without its consent by invoking section 4 (1)(b)[37] of the DPDP Act which talks about *'certain legitimate use'* under the DPDP Act which is one of the lawful ground to access the data of the employees. In the EU's GDPR one of the lawful grounds to process data is laid down under Article 6(1)(f)[38] it

[36] Arun Prabhu, Arpita Sengupta & Anoushka Soni, *India's New Data Protection Law: How Does it Differ from GDPR and What Does that Mean for International Businesses?,* CYRIL AMARCHAND MANGALDAS BLOGS (Jan. 28, 2025, 8:30 PM) https://corporate.cyrilamarchandblogs.com/2023/10/indias-new-data-protection-law-how-does-it-differ-from-gdpr-and-what-does-that-mean-for-international-businesses/; *Common Concepts in the Data Protection Laws of India and Singapore,* HERBERT SMITH FREEHILLS (Sept. 07, 2023) https://www.herbertsmithfreehills.com/notes/data/2023-09/common-concepts-in-the-data-protection-laws-of-india-and-singapore.

[37] MARDAV, *supra* note 5.

[38] EU GDPR, Art. 6(1)(f).

states that there must be a necessity and purpose for the legitimate interest ground to be invoked by the controller except in those situations where such extraction of the personal data will hamper the fundamental interest of the data subject which in our case is the employee or where such data subject is the child.[39] Herein, under the GDPR legitimate interest ground acts as an exception to consent. There is also a proviso to Article 6(1)(f)[40] which incorporates that the data which is been processed on the ground of legitimate interest cannot be invoke by the public authorities to access the personal data of the individual.

However, there are certain tests and guidelines laid down to invoke *'legitimate interest'* ground under Article 6(1)(f)[41] GDPR. The regulation incorporates under its ambit the three-part test which encompasses of *purpose test, necessity test* and *balancing test* which should be complied by the employer when invoking the exception of legitimate interest ground. *Firstly*, the purpose test states that the employer processing the data of the employees should have a valid purpose behind processing of the data for example to check whether the employee has committed any fraud or not earlier etc. *Secondly*, the necessity test here the necessity can be checked through two things together: first, if using the data helps reach the goal effectively, and second, if using the data affects employee's rights less than other ways to achieve the same goal. *Lastly*, the balancing test needs to be carried out which involves comparing the legitimate interests of the data controller (employer) and what will be the impact on the privacy rights of the data subject's (employees). By examining both sides, a tentative balance has to be determined and maintained.

It is noteworthy that whenever the employer is invoking the ground of legitimate interest under the GDPR even though the consent is not required to be taken for processing the personal data, there is an essential transparency mechanism put in place.[42] As per Article 13(1) (d)[43] of GDPR in cases where the personal data is being accessed by the data principal the information regarding the same must be provided to the employees and under Article 14 Paragraph 2 (b)[44] of GDPR where the information needs to be provided to the employees where such information regarding their personal data is not been obtained from them must be communicated to such

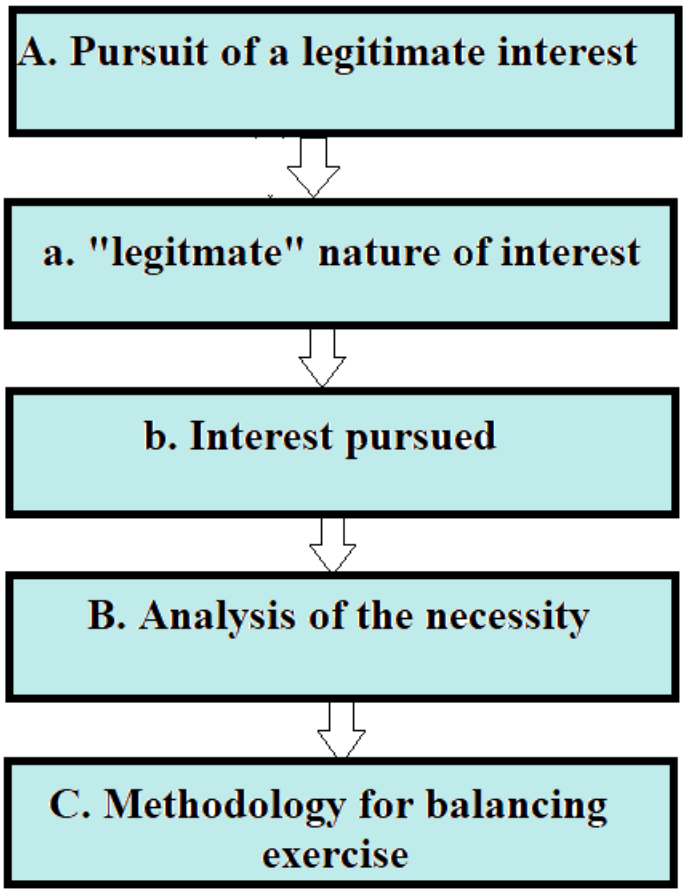
[39] Gabriela Zanfir-Fortuna & Teresa Troester-Falk, *Processing Personal Data on the Basis of Legitimate Interests under the GDPR*, THE FUTURE OF PRIVACY FORUM (2018) https://fpf.org/wp-content/uploads/2018/04/20180413-Legitimate-Interest_FPF_Nymity-2018.pdf
[40] Supra note 4.
[41] Supra note 4.
[42] Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR Version 1.0 (October 8, 2024), https://www.edpb.europa.eu/system/files/2024-10/edpb_guidelines_202401_legitimateinterest_en.pdf.
[43] EU GDPR, Art. 13(1)(d).
[44] EU GDPR, Art. 14(2)(b).

employees so to adhere to transparency and fairness procedure.[45] Also, it was stated in one of the case that *"the data subject has the right to object at any time on compelling legitimate grounds related to his particular situation to the processing of data (based on Article 14 of the Directive)."* Article 29 of the Working Party[46] states that, *"Legitimate interest"* pursued by the controller must be "*real, current, and related to ongoing activities or immediate future benefits."*

The interest should be clearly defined so that it can be weighed against the rights of the employees who are the data subject. The term legitimate means that it must be lawful and should be allowed by EU and its national law. Further on Article 29 Working Party[47] states that the first step is to carry out the balancing test here the balancing test is in furtherance to the objective which the employer wants to achieve by accessing the data of the employees and in the process the fundamental rights to have data privacy should not be hampered.

Thus, the balance has to be maintained with the objective to be achieved with the fundamental rights of the employee then only the employer can access the data of the employee by using the ground of legitimate interest. For invoking the ground of legitimate interest, all the three tests must be satisfied. If any one of these three tests is not met the threshold for invoking legitimate interest will not be sufficient and thus cannot be invoked.[48]

[45] DPDP Act, *supra* note 21.
[46] Article 29 Working Party, "Opinion 6/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46 April 9, 2014, p. 13."
[47] *Id*.
[48] CJEU-C-13/16- Rigas satiksme, ECLI:EU:C:2017:336.




Graphical representation of "Elements to be taken into consideration when assessing the applicability of Article 6(1)(f)[49]

Furthermore, Article 8(2)[50] of the Charter of Fundamental Rights of the EU states that *"on the basis of the consent of the person concerned or some other legitimate basis laid down by law"* that the data can be processed.

The EU GDPR has enacted a provision for special personal data which takes care of special category of personal data of employees. Article 9[51] talks about processing of special category of personal data where it states under Article 9(1)[52] that *"Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely*

[49] Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR Version 1.0 Adopted on 8 October 2024, https://www.edpb.europa.eu/system/files/2024-10/edpb_guidelines_202401_legitimateinterest_en.pdf.
[50] Article 8(2) of the Charter of Fundamental Rights of the European Union.
[51] EU GDPR, Art. 9.
[52] EU GDPR, Art. 9(1).

*identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited."* As a general rule under Article 9 Paragraph 1[53] accessing special category of personal data of employee is impermissible but there are few exceptions carved out to the general rule of not accessing such special category of personal data under Article 9 Paragraph 2[54]. Further on Article 9 Paragraph 2 (b)[55] states that such personal data of the special category of the personal data can be accessed by employer on grounds of *"employment, social security and social protection law."*

In addition to Article 9 of GDPR Article 88 of GDPR[56] specifically talks about *"processing in context of employment"* it states that the member states may allow by way of agreement to ensure protection of the freedom and rights of the employees with respect to processing of their personal data in context of employment which may include performance of contract of employment, recruitment, management, planning, health and safety at workplace etc. It also states that there should be suitable and specific measures which should be adopted to safeguard the human dignity, legitimate interest and fundamental rights of employees about transferring and processing of their personal data.

Thus, it can be stated that under EU's GDPR has a special framework laid down for accessing the data of the employees by the employer as it can be clearly seen that the law out there has specifically cull out that what all data can be accessed by the employer of the employee under Article 9 and Article 88 for employment purposes and if some category of data which is not been mentioned under Article 9 and if the employer wants to access such data then he can invoke the ground of legitimate interest under Section 6(1)(f)[57] for which he has to fulfil all the three threshold i.e., necessity, purpose and balancing test. Such mechanism is absent in the DPDP Act as there is no test or guidelines which are in place to deal with the ambiguity of the term for *'employment purpose'* in the DPDP Act.

**B. Comparison between DPDP Act with the PDP Act in the context of "Certain Legitimate Use" v. "Legitimate Interest"**

The PDP Act has incorporated 'Legitimate interest' exception in the year 2020 through a Personal Data Protection (Amendment) Act 202058 (hereinafter as "Amendment Act"). On

[53] *Supra* note 17.
[54] EU GDPR, Art. 9(2).
[55] EU GDPR, Art. 9(2)(b).
[56] EU GDPR, Art. 88.
[57] *Supra* note 4.
[58] The Personal Data Protection (Amendment) Act, 2020, No. 40, Acts of Parliament, 2020 (Singapore).

2nd November 2020 the Amendment Act, was passed and has incorporated number of amendments. One of the amendments made were regarding the introduction of exception legitimate interest which came into effect on 1 February 2021[59] before that legitimate interest was not a ground of exception to consent under PDP Act. [60] In PDP Act legitimate interest can be found under paragraphs 2 to 10 under Part 3 of the First Schedule of the PDP Act 2012.[61]

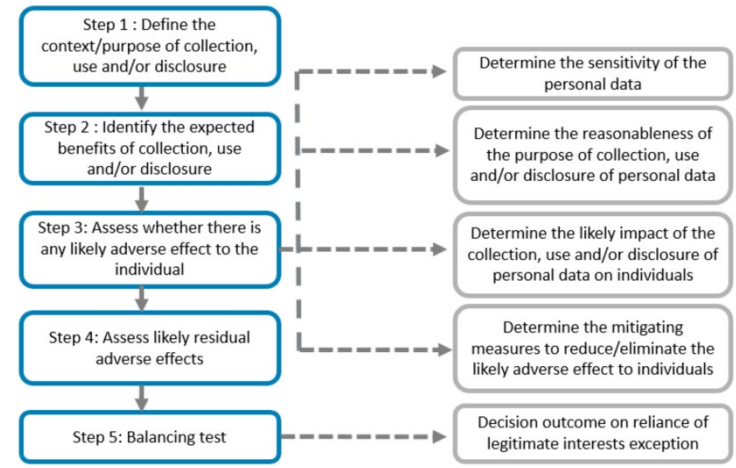
The term ***"****Legitimate interests"* exception generally refers to any lawful interests of an organization or other person (including other organizations). The exception is usually invoked by the employer to access the data of its employees without taking their consent *"where it is in the legitimate interests of the organization and the benefit to the public is greater than any adverse effect on the individual."*[62] For an organization to take the benefit of the legitimate interest exception laid down under Paragraph 1 of the Part 3 of the First Schedule[63] of the PDP Act 2012 the organization must adhere to the same[64] which lays down two condition. The first requirement is that, *"the collection, use or disclosure of an individual's personal data must be done in pursuance of the legitimate interests of the organization."*[65] The second requirement is that the organization must balance its legitimate interests for accessing the data against the interests of the individuals.[66] Also, the organization has to conduct a Data Protection Impact Assessment as per Paragraph 1(2)(a) of Part 3 of the First Schedule[67] of the PDPA which states that there must be an assessment carried out prior to *"collecting, using or disclosing the data to the third party"* here the assessment must meet the threshold laid down under Paragraph 1(1) of Part 3 of the First Schedule[68] of the PDPA. Further it also states that the individual must be given reasonable access to the information of why the organization is collecting such data.

With respect to the Data Protection Impact Assessment which the organization must carry out and which must encompass the four things essentially which is laid down under the Annex-C

[59] Wilson Ang, Jeremy Lua, Terence De Silva, *Relying on the Legitimate Interests Exception under the Personal Data Protection Act 2012*, NORTON ROSE FULBRIGHT (Mar. 28, 2023) https://www.dataprotectionreport.com/2023/03/relying-on-the-legitimate-interests-exception-under-the-personal-data-protection-act-2012/ .
[60] *Id*.
[61] The Personal Data Protection Act, 2012, Part 3 of First Schedule, Para 2-10 (Singapore).
[62] Nicole Leong, *A Practical Round-Up of Singapore Data Protection Developments In 2021*, REED SMITH (Dec.13, 2021) https://www.reedsmith.com/en/perspectives/2021/12/a-practical-round-up-of-singapore
[63] The Personal Data Protection Act, 2012, Part 3 of First Schedule, Para 1 (Singapore).
[64] The Personal Data Protection Act, 2012, Part 3 of First Schedule, Para 1(1) (Singapore).
[65] *Supra* note 27.
[66] *Id*.
[67] The Personal Data Protection Act 2012, Part 3 of First Schedule, Para 1(2)(a) (Singapore).
[68] KAVYA, *supra* note 28.

Assessment Checklist for Legitimate Interests Exception[69] where the first thing to check is the purpose, second being the reasonableness of purpose, third whether the benefits of the legitimate interests clearly outweighs any adverse effect to the individual, lastly the final decision outcome of the assessment.

Figure 1: The flow for conducting legitimate interests exception assessment




The flow chart has been taken from ***"Annexure C of Assessment Checklist for Legitimate Interests Exception 2021."*** [70]

Instance where the legitimate interest may apply is for the *"investigation relates to company employees and if the collection, use or disclosure of the personal data is reasonable for the purpose of managing or terminating the employment relationship with the individual".*[71] Paragraph 1(10) of Part 3 of the First Schedule[72] of the PDP Act has carved out an exception for employment purposes where the collection, use and disclosing the data of the individual by the organization will be termed as reasonable for the purpose of entering into an employment relationship with the individual[73] managing or terminating the employment relationship with or appointment of the individual.[74] It is thus stated that the test which is involved to invoke the legitimate interest under the PDP Act is that it must fulfil the condition like first it must check

[69]Annex-C Assessment Checklist for Legitimate Interests Exception, https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/AG-on-Key-Concepts/Annex-C--Assessment-Checklist-for-Legitimate-Interests-Exception-1-Feb-2021.
[70] *Id*.
[71] Farhana Sharmeen, Esther C. Franks, Gen Huong Tans, *GIR Know How Data Privacy & Transfer Investigations*, LATHAM & WATKINS LLP 4 (2021) https://www.lw.com/admin/upload/SiteAttachments/GIR_Data%20Privacy%20-%20Transfer%20in%20Investigations_SP.pdf
[72] *Supra* note 64, Para 1(10).
[73] *Id*., Para 1(10)(a).
[74] *Id*., Para 1(10)(b).

what is the necessity for the employer to access the personal data of the employee, second whether the collection of the data of the employee would have any adverse effect on the employee, third to identify reasonable measure which can mitigate the adverse effect, lastly to check whether the employer interest supersede the interest of the employee even though the necessary steps were taken.[75] Such mechanism is absent in the DPDP Act as there is no test or guidelines which are in place to deal with the ambiguity of the term for *'employment purpose'* in the DPDP Act.

Thus, it can be concluded by stating that when comparing the DPDP Act with the two most important legislation on data privacy of the world i.e., GDPR and the PDP Act. It is clear that how the term "legitimate interest" has been interpreted in the context of employment purpose. There are set of regulations and tests which are laid down to determine the threshold of the term legitimate interest but on the contrary under the DPDP Act there is no threshold laid down for the interpretation of the term "certain legitimate use" and "for employment purpose" what all can constitute under the said terms thus makes it ambiguous and vague.

The ambiguity may lead to multiple interpretations of the terms which in turn may lead to violation of Article 14[76] and Article 21[77] of the Constitution of India. Article 14[78] will be violated as in the DPDP Act the sole power is been given to the employer to decide what will classify as employment purposes which will lead to arbitrariness and unbridled power. Simultaneously this will lead to the violation of Article 21[79] because as discussed earlier, the Act does not provide adequate safeguards for protection of employee's data and the DPDP Rules are silent about any procedural requirements for the same.

This is also antithetical to various international instruments such as the ICCPR and UDHR which recognize the right to privacy.[80] The general comment on Article 17 of the ICCPR too talks about the need to discourage arbitrary interference with privacy.[81] The right to privacy has recently been affirmed by the United Nations General Assembly Resolution on Privacy,

[75] RedMart Limited [2023] SGPDPC 1, https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Commissions-Decisions/Decision---RedMart-Limited---18012023.pdf
[76] INDIA CONST. Art.14.
[77] INDIA CONST. Art. 21.
[78] *Supra* note 48.
[79] *Supra* note 49.
[80] UN General Assembly, *Universal Declaration of Human Rights*, Article 12, 217 A (III), 10 December 1948, https://www.refworld.org/legal/resolution/unga/1948/en/11563, UN General Assembly, International Covenant on Civil and Political Rights, United Nations, Treaty Series, vol. 999, p. 171, 16 December 1966, https://www.refworld.org/legal/agreements/unga/1966/en/17703.
[81] *Id.*

wherein proportionality of measures interfering with privacy has been discussed.[82] The Indian Supreme Court has often read these international instruments as a part of the domestic law and therefore, the government is under the obligation to abide by them.[83] A data protection legislation which respects employee's privacy is the thus the need of the hour.

**4. The Way Forward**

Through the elaborate discussion in Part III, it can be said that the data protection legislations in European Union and Singapore have adopted an extensive framework for collection of employee's data. This ensures transparency, and respect for principles for data collection. However, as we have discussed in the article, the same level of protection is lacking in India. Additionally, the relevant section suffers from ambiguity which makes it prone to misuse leading to privacy harms and since right to privacy is a fundamental right there are constitutional repercussions arising out of the same.

While, the authors concur with the observation of B.N. Srikrishna Committte Report that employers need to have provision that provides them with relief from burdensome data processing, this must be done with adequate protection mechanism.

We propose the following measures to be taken by the legislature to protect workers privacy based on our analysis of India's data protection framework and drawing from the recommendations made by various entities such as the International Labour Organisation and Data Security Council of India.[84] We also rely on the guidance provided in other jurisdiction with regards to processing and collection of data at workplace.[85]

---

[82] Right to Privacy in the Digital Age, https://digitallibrary.un.org/record/3896430?ln=en&v=pdf.

[83] Navtej Singh Johar v. Union of India, (2018) 1 SCC 791, Indian Young Lawyers Association & Ors. v. The State of Kerela and Ors., 2019 (11) SCC 1.

[84] Frank Hendrickx, *Protection of Workers' personal data: General principles*, INTERNATIONAL LABOUR ORGANIZATION (Jan. 25, 2025, 3:30 PM) https://webapps.ilo.org/static/english/intserv/working-papers/wp062/index.html; Abha Tiwari, *Privacy sat the workplace- A practical guide to Ethical employee data management*, DATA SECURITY COUNCIL OF INDIA, PRIVACY LEADERSHIP FORUM (Jan. 28, 2025, 4:30 PM) https://www.dsci.in/files/content/documents/2024/Privacy-at%20-the-Workplace-DPLF-SIG-paper.pdf; ELECTRONIC PRIVACY INFORMATION CENTER, *Workplace Privacy* https://epic.org/issues/data-protection/workplace-privacy (last visited Jan. 24 2025); Dhruv Somayajula and Ameen Jauhar, *Retaining informational privacy in the age of emerging technology*, VIDHI CENTER FOR LEGAL POLICY (February, 2022) file:///C:/Users/VENDORS/Downloads/20220214_Retaining-informational-privacy-in-the-age-of-emerging-technology.pdf.

[85] Office of the Personal Data Protection Inspector, 'Recommendations regarding personal data protection in labour relations', file:///C:/Users/VENDORS/Downloads/Recommendations-Regarding-Personal-Data-Protection-in-Labor-Relations-.pdf,
Information Commissioner's Office, 'Employment Practices and data protection monitoring workers' https://ico.org.uk/media/for-organisations/uk-gdpr-guidance-and-resources/employment-information/employment-practices-and-data-protection-monitoring-workers-1-0.pdf

**Suggestions**

a. The Act must incorporate the principles of data processing and collection as recognised by the OCED, APEC and the United Nations, making Indian law compatible with the international framework.

b. The Act must mandate that any data collection and processing must comply with the threefold requirement of necessity, proportionality and legality as upheld in Puttaswamy.

c. Pursuant to the above suggestion, the Act and rules must incorporate a detailed test for pursuing 'legitimate use' like the GDPR as discussed in Part III of this pape.

d. The Act must provide an inclusive description of the term - 'employee'. This description must include platform workers, interns, and persons on probation, former employees, and persons interviewed for job et cetera.

e. The Act must also remove the ambiguity in Section 7(i) by limiting the scope of the term – 'employment purposes'. The scope must be restricted and only cover data collection and processing which is necessary and in consonance with the privacy principals. Such limitation can be incorporated in the Act by following the example of Singapore's data protection law which has prescribed the limited circumstances in which the data can be processed.

f. It is also required that various provisions of the Act as discussed in Part II (A) of this paper are amended to include collection and processing of data under Section 7(i) thus giving the Data Principals the right to know the purpose of collection and the data which is being collected.

g. It also required that the Act provides for the right to erasure of data and limitation on the period of retention of data when being collected and processed pursuant to Section 7(i). The current prescription to retain the data as per the assumption of reasonable use is prone to misuse.

h. The Act must also prescribe a mechanism for data processing impact assessment. This will align India's Privacy law with other leading privacy laws and ensure transparency and accountability.

i. The DPDP Act does not contain a provision for processing of sensitive personal data including biometric data. Other jurisdictions such as the EU, the UK and Singapore have

such provision which in turn prescribes a higher threshold for processing of such kind of data given its impact on the data principal. The same must be incorporated within the DPDP Act.

j. The current legislation also does not regulate the use of automated decision making, leaving data prinicpals to the arbitrary decisions of the artificial intelligence tools without any scope of human oversight.

**5. Conclusion**

It is true that flow of information is playing and will be instrumental in the growth of our economy however such growth should not disregard the right to privacy. Since privacy is not only a cherished value but it is also integral to human dignity.[86] This is also applicable to the myriad people who engage in one form of employment or the other. The need for livelihood should therefore not result in the breach of privacy by the employer. Use of invasive monitoring not only degrades privacy but also reduces the trust of employees thereby proving counterproductive to the goal of enhancing efficiency of output.[87] Therefore, necessary steps must be taken by the employers made to keep this right intact. The law should also play a crucial role in ensuring that the right to privacy is protected and not breached.

Through this article, the authors have tried to contextualize the need to secure employee's right to privacy amidst the increase in the use of surveillance tools and other invasive technologies. The authors have also tried to highlight the shortcoming of the DPDP Act in this regard by doing and intra and inter-comparative study with the previous Bills and the legal framework of the European Union and Singapore respectively. The authors have particularly emphasised on the significance of laying down a threshold for processing under the ground of 'legitimate interest' and restricting the scope of 'employment purpose under the DPDP Act'. Adopting this measure would curb arbitrary collection and processing of data by the employers. Additionally, the authors have highlighted other gaps in the DPDP Act which may adversely affect the privacy of the employees. Suggestions to this end have been made towards the end of this paper.

[86] LUCIANO, *Supra* note 1, at 311.
[87]Daniel M. Ravid, Jerod C. White, David L., Tara S. Behrend, A meta-analysis of the effects of electronic performance monitoring on work outcomes, Wiley Online Library, (2022), https://doi.org/10.1111/peps.12514; KRISTIE, *supra* note 3.