INFERRED DATA AND SILENT SURVEILLANCE: A DPDPA PERSPECTIVE

Sneha R Iyer, Senior Corporate Counsel at Newton School

ABSTRACT

Consent frameworks in data privacy largely revolves around data collected directly from an individual and rarely around inferred data such as the personality traits, spending capacity, buying preferences, health status etc. This poses a huge threat to personal freedom as non-consensual inferring of data results in rigged algorithms, vulnerability targeting and manipulation of consumer choice. It is no longer a breach of consumer rights; it is severe case privacy and dignity breach. Organisations processing these sensitive data in the guise of providing better and customised services to the users, are majorly for business profitability. From ensuring that users are retained within the brand to creating a dependency by satisfying needs even before they arise; organisations are truly benefiting from this 'unethical' processing.

The paper delves into the concept of data profiling and the legality which govern such practices in India. The paper further covers what 'ethical data profiling' looks like and how by being aware of the rights as data holders, people can exercise greater control over their personal data. The paper focuses on the Digital Personal Data Protection Act, 2023 and how it is set to empower Indian citizens to hold organisations answerable and accountable for their personal data. Furthermore, the paper refers to the European regulations relating to data protection in order to provide the readers with an international perspective of data profiling, its legality and ethical usage. In this fast-paced-era, where every Minuit detail of one's existence is being processed by Artificial Intelligence models, the adoption of a 'well-regulated-data-protection-regime' by India will change the whole landscape of how privacy and dignity is viewed.

Key Words: *- Digital Personal Data Protection Act, 2023, Privacy, Targeted Advertisements, Data Profiling, GDPR, Bundled Consent, Inferred Data, Rights of Data-Principal*

I. INTRODUCTION

With the advent of the Digital Personal Data Protection Act, 2023 (hereinafter referred to as 'DPDPA'), India is witnessing an increase in its citizens actively speaking up about their rights when personal data is being collected. People are reading the Terms and Conditions more often, raising requests for deletion of data, telling the billing agent at the nearby shop that we don't want to give our phone number and email, asking the sales agent on spam calls to confirm their allegiance before giving out any personal data, and so on. This shift was initially evident at the time of Puttaswamy judgement[1], but the enactment of the DPDPA gave citizens a strong, clear foundation to enforce their rights. But are the visible data collection and processing, the only processing done by organisations? What about the data that is processed without our knowledge? What about the data inferred from our personal data? Did we really consent to the processing? Let us look into it.

II. WHAT IS INFERRED DATA OR PROFILING OF PERSONAL DATA?

When we get targeted advertisements orproduct recommendations, or receive promotional/sales calls for purchase requirements, we would think, "How did they know exactly what I want?". The truth is the data we provide while creating a profile on a website or app, or while making a purchase; or while removing certain items from our cart;or while moving certain items to a wish-list; or while answering a pop-up question saying; or while givingfeedback after using a product or service; are no longer used merely as mechanisms to enhance the product/service's performance or quality. It is also silently understandingand analysing our purchase preferences, our spending trends,lifestyle choices and many actions which are deeply personal to us.[2]

This is nothing but the inference of personal data and, in many cases, the 'profiling'[3] of personal data.

[1] Justice K.S. Puttaswamy (Retd.) and Anr. vs. Union of India and Ors,(2017) 10 SCC 1
[2]David Alexander and Amelia Ethan, 'Designing Customer-Centric Products Using AI-Powered Behavioral Analytics and Feedback Loops', Volume 12 Issue 01, Journal of Artificial Intelligence in Medicine, pg.656 (2021).
[3]"Profiling" means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements, art 4(4), General Data Protection Regulation, 2016.

This is either done manually by employees of companies, by analysing large data sets, or done via AI tools that closely monitor each of our actions on the website or app; and send analysed notes to the business on our behavioural patterns, preferences, financial health, and expectations. The routine feedback or the tabs we explore while shopping is helping the business understand our needs and capacity, and thereby are able to provide us with exactly what we need.

III. HOW LEGAL IS THIS DATA PROFILING?

While there is no particular law like GDPR that explicitly calls out profiling and inferred data, the DPDPA does govern this aspect of data handling. The Act defines personal data as data that is identifiable to an individual.[4]If the profiling is done so that it can be traced back, directly or indirectly, to a person, it becomes difficult to argue that it falls outside the scope of personal data. Hence, this means organisations ought to seek consent before profiling data.

Organisationsmay argue that we have taken bundled consent from the data principal to process the personal data for analytics purposes. The real question is whether the notice of using the personal data for analytics and profiling is hidden somewhere in a 20-page Terms and Conditions constitutes as a valid notice. And whether accepting the T&C suffices as consent? DPDPA explicitly prohibits bundling of consent. Under Section 6, valid consent needs to be free, specific, informed through a clear affirmative action by the data principal.[5] Bundling of consent and hiding important notices like profiling through a T&C is no longer legally valid[6]; the person needs to be fully aware of what they are consenting to.The Act mandates consent to be free, specific, informed, and unconditional.[7] Therefore, bundled consent or hidden disclosures will not be a valid consent for processing data. This is a very important aspect of the DPDPA Act, as it aims to give individuals a high level of control over their personal data being processed. Organisations must also keep in mind that use of AI tools for profiling data will not exempt organisations from the compliance under the DPDPA, as the scope of the act is broader than what many organisations perceive; as it covers the processing of *'any'*digital personal data irrespective of the medium or tool of processing.

[4]The Digital Personal Data Protection Act, 2023 (Act 22 of 2023), s. 2(t).
[5]The Digital Personal Data Protection Act, 2023 (Act 22 of 2023), s. 26.
[6]Explicit Consent Under India's DPDP Act: Best Compliance Practices, available at https://www.idfy.com/blog/explicit-consent-under-indias-dpdp-act-best-compliance-practices/ (last visited on May 19, 2026)
[7] Supra Note 6 at 3.

IV. THE DEFENCE OF ANONYMISATION

Organisations are largely advocating that the data has been anonymised and cannot be traced back to any individual; hence in such a scenario, the profiling of data is not a significant concern.[8] If the data is anonymised, then how are the organisations able to target customers with particular products that they are in need of, even before they have showcased their requirement? Maybe the profiling is not really done on anonymised data, but rather is done on pseudo-anonymised data. Pseudonymization[9] allows re-identification with a secure key, whereas Anonymization[10] is irreversible as it permanently removes the identifier. Hence, if the data is not fully anonymised and the profiled data can still be tracked back to the individual the personal data comes under the purview of the DPDPA and the consent mechanism.

V. CONCLUSION

Theissue is no longer whether silent surveillance exists, but whether, we are proactively vigilant and careful in our day-to-day activities involving our personal data. As one fictional warningaptly captures: "*In Today's India, the currency of identity, control and power is no longer grains and gold- but data. Those who lose control over it, end up surrendering their identity and freedom; as privacy breach is a breach of dignity*".[11]

The DPDPA aims to empower theIndian citizens by giving them better control over their personal data. From purpose-specific consent requirements to right to withdraw consent[12], individuals can now choose how and for what purpose their personal data is collected and processed. Individuals also have the right to seek detailed information[13] on what data is processed, the manner of processing, the retention practices among other things[14], in a clear and understandable manner. Data protection is no longer technical or legal concept requiring a legal expert to intervene, but is becoming self-reliant mechanism through which you canhave a control over your data in the modern digital world.

[8]Teesha and Dr. Dhawal Shankar Srivastava, 'Data Anonymisation, The Right to Explanation, and The Architecture of Accountability under The Digital Personal Data Protection Act', Volume I, HILSR Law Review, page 93 (2025),
[9]General Data Protection Regulation, 2016, art 4(5).
[10]General Data Protection Regulation, 2016, recital 26.
[11]The Long Run: A Tale of the Continuing Time, *available at:* https://www.goodreads.com/work/quotes/1416-the-long-run (last visited on May 14, 2026)
[12]The Digital Personal Data Protection Act, 2023 (Act 22 of 2023), s. 6(4).
[13]The Digital Personal Data Protection Act, 2023 (Act 22 of 2023), s.11.
[14]The Digital Personal Data Protection Act, 2023 (Act 22 of 2023), s.12, s.13 & s.14.