INFORMATIONAL SELF-DETERMINATION TO DIGITAL PRIVACY: COMPARING GERMANY AND INDIA

Abhijith A. S
Dual Degree Master's LL.M. Student,
National Forensic Sciences University,
India and Tashkent State University of Law, Uzbekistan
https://doi.org/10.5281/zenodo.21187494

Abstract

This article checks how the legal frameworks of India and Germany handles data protection and privacy issues by analysing their legal history which also includes their constitution so as to show how the law developed as it is connected to the developing digital realities. We can clearly see that the German Constitution recognises right to privacy as a very important constitutional right and the Federal Constitutional Court also recognised the right to determine, how and when one wants to share personal information. The data privacy law of Germany deeply influenced other European countries to make similar laws and this also led to the demand for the creation of the General Data Protection Regulation.

Coming to India, the Supreme Court through the case Justice K.S. Puttaswamy (Retd) v Union of India, 2017 recognised privacy as a fundamental right and held that privacy falls under Article 21 of the Indian Constitution. This also led to the enactment of the Digital Personal Data Protection Act of 2023. The Indian approach with respect to protection of data and privacy makes the data-fiduciary model to create a balance between the individual rights and interests in the fast growing digital economy.

Keywords: Informational Self-Determination, Data Protection, Privacy, Federal Constitutional Court, General Data Protection Regulation, Digital Personal Data Protection Act

I. Introduction

In this current world, data has become an important part of one's digital presence. With the move towards algorithmic management of our lives, laws and regulations that have been created to govern what we do and the information we produce on a daily basis vary significantly by country.[1] The aim is to compare two different types of data protection regimes, Germany being the first one considered as the leaders in continental European law on privacy and next one the fast growing digital giant, India. Coming to Germany's privacy system, it has developed out of its' post second world war protection of human dignity and people's personal autonomy, but India's policy was to establish a different approach moving from a government lead digital public infrastructure to a constitution based on rights.[2]

Germany's foundational data privacy laws are based upon the 1983 Census Ruling given by Germany's Federal Constitutional Court. This ruling was given as there was too much intrusion from the side of the government into the lives of the people. The court

[1] Kolanu, M., Lakra, R., & Shrivastava, A. (2026). Data, control and power: Decoding India's Digital Personal Data Protection Act, 2023. Global Privacy Law Review, 6(4), 136–155

[2]Patra, L. (2026). Digital Personal Data Protection Act, 2023 and the vision of Viksit Bharat@2047: Towards sustainable digital governance and inclusive growth in India. Journal of Social Review and Development, 5(1), 88–101

established the right to informational self-determination which meant that, the people had the right to choose how, when and whether to disclose their private lives.[3] This principle confirmed that privacy violations resulted in significant changes in the human behaviour and threatened the existence of a free and democratic society. Therefore, the Census Ruling can be seen as the foundation which led to development of national laws of Germany with respect to data privacy. This was also used as the framework for GDPR in the European Union, that considered protecting data as an important right of the humans.[4]

The digitalization that happened across the economy of India and the widespread expansion of the Aadhaar's biometric ID system led to the legislative development of India. The most important event was the decision given by the Supreme Court in *Justice K.S. Puttaswamy (Retd) v Union of India (2017)*.[5] The court ruled that right to privacy falls under Article 21 of the Constitution of India.[6] The decision given by the court led to the enactment of the Digital Personal Data Protection (DPDP), 2023. So, when we compare the right to control one's information established by Germany with the new data protections laws of India we can see that both the countries play an important role in balancing the rights of citizens and the authority of the government in the digital space. So the main research question which this article put forwards is, to what extent does India's Digital Personal Data Protection Act, 2023 align with or diverge from the German constitutional doctrine of Informational Self-Determination?

II. Materials and Methods

The paper employs a qualitative, historical-doctrinal and comparative legal analysis. Rather than deploying empirical data collection which includes surveys and statistics, the methodology relies on analysing foundational legal texts, landmark judicial precedents and statutory frameworks from Germany and India. The paper reaches its conclusions by examining and comparing primary as well as secondary legal sources from the two different jurisdictions:

With respect to Germany, the analysis was based on Articles 1(1) which talked about human dignity and 2(1) about personality from the Basic Law of Germany. It heavily evaluates judicial material from the landmark 1983 Census Act Ruling by the Federal Constitutional Court, as well as the downstream statutory manifestation in the European Union's General Data Protection Regulation (GDPR).

Coming to India Section 43A of the Information Technology Act, 2000 and the Sensitive Personal Data Rules, 2011 were analysed. The primary modern materials consist of the Supreme Court's decision in Justice K.S. Puttaswamy (Retd) v Union of India (2017), the Justice B.N. Srikrishna Committee Report (2018) and the codified Digital Personal Data Protection Act, 2023.

[3]Vivarelli, A. (2020). The crisis of the right to informational self-determination. The Italian Law Journal, 6(1), 301–318

[4] Schmidt, K., & Laje, A. (2016). The proportionality and solidarity principles and their impact on privacy laws in German jurisprudence. Laws, 5(2), Article 27

[5] Justice K. S. Puttaswamy (Retd.) v. Union of India, 10 SCC 1 (2017)

[6] Article 21, The Constitution of India, 1950

III. Results

1. German Doctrine of Informational Self-Determination

According to the legal system of Germany, individual's personal data is inseparable from an individual's own physical being. This is the main reason behind establishing right to protect one's data as a fundamental defensive right against the overreach by the private and government entities. The data privacy of Germany has its structural foundations in its constitution itself. Even though the words data protection and privacy were not used in the constitution, the Federal Constitutional Court of Germany used two separate provisions given in the constitution to totally establish a new and independent right known as the General Right of Personality.[7] These two provisions are:

1. Article 1(1)[8] - human dignity is considered important and tells that every state authority has the duty to respect and protect human dignity.

2. Article 2(1)[9] - guarantees that, people are free to live their life as per their choices and can frame their personality as per their own wish in a way not causing harm to others.

These provisions were combined together and later it was established that to protect human dignity, there should be ultimate control by the individual with respect to how his or her persona is presented and treated by the society.

During the year 1983, December 15 the West German National government decided to conduct a national census but, due to the complaints raised by more than 34,000 German citizens with respect to the way they collected the personal data when consent was not given by them. This date changed at the international level the privacy law's history.[10] On June 15, 1983 the Constitutional court gave its decision regarding the method in which the data is collected and recognised that every person has the right to privacy and also stated that the without the consent of the individual the government cannot collect, use or store the personal data.

2. India's Journey from Aadhaar to DPDP Act

If we go through the history, we can see that before 2017 in order to protect one's privacy rights there was no single legal framework and the only way of protecting the digital data was possible through Section 43A of the Information Technology Act, 2000. There was only limited protection that could be provided to the Indian citizens through the Sensitive Personal Data Rules, 2011 and it applied only to the corporate entities. In fact there was no legal framework that was in force to limit the surveillance done by the state or the data aggregation. Then the Aadhaar Project came into being which was brought by the Unique Identification Authority of India. This was developed as an administrative tool that could deliver welfare payments to the citizens. However, it became a widespread way to create identity for everyone in India through the use of demographic information and biometric identifiers. The representatives of the Indian government argued that individual's privacy right is not specifically afforded to them by way of constitutional rights.

---

[7] The birth of informational self-determination: 40th anniversary of the German "census judgment." (2023, December 15). GDPR

[8] Article 1(1), Basic Law for the Federal Republic of Germany, 1949

[9] Article 2(1), Basic Law for the Federal Republic of Germany, 1949

[10] The birth of informational self-determination: 40th anniversary of the German "census judgment." (2023, December 15), GDPR

Everything changed with the decision given by the Supreme Court through the case *Justice K.S. Puttaswamy (Retd) v Union of India*[11] in which the right to privacy was established and it was also held that right to privacy also refers to right of life and right to personal liberty given under Article 21 of the Constitution of India. It was also stressed through the case that informational privacy is an essential part of individual autonomy. In the digital world, personal information stands as an extension of the person and the individual enjoys the right to control the dissemination, retention and processing of their personal information. The Supreme Court also established a strict, three-pronged test of proportionality to guide all state intrusions into an individual's right to privacy and to guard against excessive state encroachment into ones privacy.

The test includes three components:[12]

LEGALITY	The intrusion into one's privacy must be supported by a statutory law.
LEGITIMATE STATE	The state must have a valid purpose for the intrusion which may include national security or welfare distribution.
PROPORTIONALITY	The means used to effect the intrusion must be the least intrusive and most reasonable to achieve the objective, with the presence of built-in procedural safeguards to protect the individual's right to privacy.

Figure 1 - Explains the three components of the test of proportionality established by the Supreme Court.[13]

3. Codification of the Digital Personal Data Protection Act, 2023

The Indian government, in response to the Puttaswamy case and due to the recommendations made by the Justice B.N. Srikrishna Committee Report (2018)[14], has passed the Digital Personal Data Protection Act in the year 2023. The Digital Personal Data Protection has been implemented through the DPDP Rules.

This act provides a much simpler data protection regime compared to the European Union's General Data Protection Regulation (GDPR). The Act consists of a unique linguistic framework:[15]

---

[11] Justice K. S. Puttaswamy (Retd.) v. Union of India, 10 SCC 1 (2017)

[12] Aashika, U. H. (2026, April 30). Beyond thumbprints: Legal challenges of biometric data protection under India's DPDP Act 2023. Record of Law.

[13] Established by the Supreme court through Justice K.S. Puttaswamy v Union of India, 2017

[14] The Justice B.N. Srikrishna Committee during the year 2018 submitted its report with respect to data protection laws in India. The commission was created after the Puttaswamy judgment which framed the draft version of the Personal Data Protection Bill.

[15] https://www.dpdpa.com/dpdpa2023/chapter-3/section11.html

Data Principal - The individual whose digital personal data is processed.

Data Fiduciary - Agency that can be public or private which makes the decision on how, when and why to process the data.

Data Protection Board of India (DPBI) - The quasi-judicial organisation appointed by the executive to promote compliance with the DPDP Act and deal with complaints.

3.1 Key Elements

The DPDP Act has formalised certain components of every Data Principal's right to be in control of their digital information through -

- **The Consent and Notice Framework** - As per the Sections 5 and 6, it is required that before the processing of data takes place there should be explicit and revocable consent which should be obtained from the Data Principal and there should be accessible and clear notice which should describe about the collected data and for what purpose it will be used for.[16]

- **The Right of Access to and Correction of Information -** According to Sections 11 and 12, the Data Principal has the right to know to whom their data has been shared and they also enjoy the right to make request in case of any corrections or when their data gets deleted.[17]

3.2 Weaknesses

Though the DPDP Act represents a significant step forward in legislative history, legal experts note that India will not fully implement an informational self-determination model due to certain weaknesses. They are -

- Section 17 states that the government can exempt any of its agencies from the act on the basis of defined and non-defined factors like national security, sovereignty and public order.[18] Some people strongly believe that this leads to the violation of the proportionality test established in the K. S. Puttaswamy case.

- Absence of Regulatory Authorities: The Data Protection Authorities in Germany and the European cannot be compared with the Data protection Board of India as it is subordinated to the executive branch as the Central Government establishes the members and terms of the body.

- Digital Literacy Gap: The Digital Personal Protection Act depends substantially on notice and consent. The point to note is that there is a widespread digital illiteracy.[19] Some

[16] Section 5 and 6, The Digital Personal Protection Act, 2023

[17] Section 11 and 12, The Digital Personal Protection Act, 2023

[18] Section 17, The Digital Personal Protection Act, 2023

[19] Gour, H. (2025, November 15). India's new Digital Personal Data Protection Rules, 2025: A Detailed Reading. https://theleaflet.in/explainer/indias-new-

critics still doubt that whether the individuals can provide consent or not or whether they will provide their tick as a sign of consent.

3.3 Similarities and Differences in Both Systems

Aspect	Germany (GDPR & Constitutional Framework)	India (DPDP Act, 2023)	Comparison
Consent	Processing of personal data is primarily based on freely given, specific, informed and unambiguous consent of the data subject.	Processing of personal data is also primarily based on free, informed, specific and unambiguous consent of the Data Principal.	**Similarity:** Both frameworks recognize valid consent as the primary legal basis for lawful processing of personal data.
Individual Rights	Data Subjects are granted enforceable rights such as access, correction, erasure and objection to processing, reflecting the constitutional principle of informational self-determination.	Data Principals are granted statutory rights, including the right to access information, correction, erasure, grievance redressal and nomination.	**Similarity:** Both frameworks empower individuals by providing enforceable rights over their personal data.
Scope of Application	Applies to both digital and non-digital (analog) personal data that form part of a structured filing system, in addition to automated processing.	Applies only to digital personal data, including data collected offline that is subsequently digitized. Purely non-digitized records are outside the scope of the act.	**Difference:** Germany provides broader coverage by regulating both digital and structured analog records, whereas India regulates only digital personal data.
Relationship Between Individual and Data Handler	The Data Controller processes personal data subject to the rights of the data subject and the regulatory obligations under the GDPR. The relationship is primarily rights-based.	The Data Fiduciary, under Section 8 of the DPDP Act, owes a fiduciary duty to process personal data in the best interests of the Data Principal, creating a quasi-trust relationship.	**Difference:** Germany follows a regulatory controller–data subject model, whereas India adopts a fiduciary model emphasizing the duty of care owed by the Data Fiduciary.
Government Exemptions and National Security	Government agencies, including intelligence and law enforcement authorities, are subject to strict constitutional safeguards. Any restriction on privacy must satisfy the principles of legality, necessity and proportionality under the Basic Law.	The Central Government may exempt any instrumentality of the State from certain provisions of the DPDP Act in the interests of sovereignty, integrity, security of the State or public order.	**Difference:** Germany subjects national security measures to stringent constitutional review, whereas India's exemption provisions grant comparatively broader discretionary powers to the Government, potentially enabling wider surveillance.

Table 1 - Explains in detail the similarities and differences in both the systems.

IV. Discussion

A comparative review of the data protection frameworks in India and Germany shows the fundamental differences between the two paradigm shifts regarding the safeguarding of human autonomy in our digital world. Germany's legal framework based on the Basic Law and the 1983 Census ruling has defined informational self-determination as an absolute right of defence for individuals giving them full sovereignty over their digital as well as analogue data as well as requiring strong, independent regulatory oversight of their data, with limited exceptions. India's current legislative framework under the Digital Personal Data Protection Act, 2023 constitutes an entirely different conceptual framework by conceptualising personal data not as an individual right but rather as a data fiduciary framework where an individual's personal data is treated as a socially shared managing economy. Through the Puttaswamy case, holding that privacy was a fundamental right under Article 21, the 2018 DPDPA has structurally diverged from Germany's absolute rights concepts because it applies solely to digital data, permits wide-ranging state exemptions from surveillance in Section 17, is subordinate to the executive branch through its regulation of its Data Protection Board of India and shifts a disproportionate burden of compliance onto a large population that has a significant digital literacy gap. As a result, Germany maintains a human-centric shield focused on individual dignity whereas, India has created a framework that favours the executive and is focused on development of India's digital public infrastructure.

---

digital-personal-data-protection-rules-2025-a-detailed-reading

V. Conclusion

The comparative analysis of legal and historical systems in India and Germany reveals that although both countries follow similar global standards for protecting digital data, there remains a stark difference between them in terms of their legal philosophies and practical application of those philosophies. Germany's model provides individuals with a strong human-based protection for their personal information that is, Germany considers personal information to be an extension of an individual's human dignity and physical being. Germany also has a strong legal framework to protect individuals against government or corporate abuses of power regarding the collection of their personal information through its Constitution. India's approach to protecting digital information is state-driven with a focus on developing economic opportunities and balancing the constitutional rights of its citizens with its fast growing digital economy and vast Digital Social Welfare Program.

Following a long history of legislative shortcomings around privacy and the state's historical claim of developmental sovereignty over the biometric Aadhaar initiative, the Supreme Court of India found that people have a legal right of privacy under Article 21 of the Constitution. The ruling in Justice K.S. Puttaswamy in 2017 established a three-pronged test for determining whether a law impinges upon individual privacy rights which must be proportionate to a legitimate state objective. However, the Digital Personal Data Protection Act of 2023 has shifted the legislative landscape from protecting individual's belief in personal sovereignty or individual dignity as a property right to creating new types of commercial data fiduciary relationships, which defines the processing or handling of personal information as a form of quasi-trust. This paper serves to highlight that while India does not simply imitate Germany or Europe with peering data protection and privacy regulations, it has modified the underlying principles of how it shall provide protections for individual's rights to privacy taking into account its own domestic socio-economic models. While Germany has been more successful in using the right to individual dignity as an absolute legal right to protect the individual from state action, India has put in place far more flexible frameworks that are more executive friendly and place more emphasis on providing regulatory efficiency and furthering the advancement of digital technologies and economies, by utilizing the existing resources of the state to support the advancement of digital economies.

Bibliography

1. Ahmed, S. (2026). Stakeholder perceptions of India's DPDP Act 2023. Frontiers in Sociology, 11, 1–15.
2. Kolanu, M., Lakra, R., & Shrivastava, A. (2026). Data, control and power: Decoding India's Digital Personal Data Protection Act, 2023. Global Privacy Law Review, 6(4), 136–155.
3. Nayyar, A. (2025). How the Indian Government Interprets Informational Privacy. Privacy Studies Journal, 4, 124–142.
4. Patra, L. (2026). Digital Personal Data Protection Act, 2023 and the vision of Viksit Bharat@2047. Journal of Social Review and Development, 5(1), 88–101.
5. Satyanarayana, P. (2024). K.S. Puttaswamy v Union of India to Data Protection. Anusandhanvallari, 4(2), 112-124.
6. Schmidt, K., & Laje, A. (2016). The proportionality and solidarity principles and their impact on privacy laws in German jurisprudence. Laws, 5(2), Article 27.
7. Vivarelli, A. (2020). The crisis of the right to informational self-determination. The Italian Law Journal, 6(1), 301–318.

8. Justice K. S. Puttaswamy (Retd.) v. Union of India, 10 SCC 1 (2017).
9. The Constitution of India, 1950, Article 21. https://www.legislative.gov.in/constitution-of-india
10. The Digital Personal Data Protection Act, 2023, Sections 5, 6, 8, 11, 12, & 17. https://www.meity.gov.in/
11. Basic Law for the Federal Republic of Germany, 1949, Articles 1(1) & 2(1). https://www.gesetze-im-internet.de/englisch_gg/englisch_gg.html
12. Aashika, U. H. (2026, April 30). Beyond thumbprints: Legal challenges of biometric data protection under India's DPDP Act 2023. Record of Law.
13. Gour, H. (2025, November 15). India's new Digital Personal Data Protection Rules, 2025: A Detailed Reading. The Leaflet.
14. Justice B.N. Srikrishna Committee (2018). Report on data protection laws in India.
15. Lissens, S. (2024). Foundations of EU personal data protection law: Privacy and Human Dignity. EU Renew Research Institute.
16. GDPR (2023, December 15). The birth of informational self-determination: 40th anniversary of the German census judgment.