LEGAL AND CONSTITUTIONAL CONFLICTS: DPDP ACT VS RIGHT TO INFORMATION ACT WITH SPECIAL REFERENCE TO INDIA AND THE UK

KM Vinita, Dr. Bhimrao Ambedkar University, Agra
Faculty of Law, BSA College, Mathura

ABSTRACT

The right to information enables individuals to access information that is legitimately available in the public domain, thereby promoting transparency and accountability. In contrast, the right to privacy protects an individual's ability to control how their personal information is collected, used, and shared. Although these two rights often complement each other, situations frequently arise where the demand for information conflicts with the need to protect personal privacy. In India, concerns surrounding data protection have existed for a long time. The enactment of the Digital Personal Data Protection Act, 2023 represents a significant development in strengthening the right to privacy. The Act places "consent" at the centre of data processing activities and recognises the principle of informational self-determination. It also seeks to enhance transparency and accountability by clearly defining the rights and responsibilities of the "Data Principal." A notable change introduced by the DPDP Act is the amendment to Section 8(1)(j) of the Right to Information Act, 2005 through Section 44(3). This provision relates to the exemption from disclosure of personal information. The amendment has the effect of broadening this exemption, making privacy a stronger ground for withholding information. Earlier, the provision allowed disclosure if a larger public interest justified it; however, the revised version has been criticised for weakening this safeguard. Civil society groups have expressed concern that this change may dilute the effectiveness of the RTI Act by giving greater weight to privacy over transparency and public interest. In this context, the present study seeks to examine the implications of this amendment and analyse it comparatively with frameworks such as the GDPR 2018 and the Freedom of Information Act, 2000.

Keywords: Digital Data, Exception, Public Interest, Disclosure, Processing, Collection

1. Introduction

Over the past few decades, the nature and importance of information have changed dramatically. Earlier, information was mainly seen as a tool to acquire and manage other resources. Today, however, it has become a valuable resource in itself and plays a central role in everyday life. In this digital age, protecting one's private space has emerged as a continuing challenge. From earlier times, individuals have struggled to safeguard their personal information and maintain control over their private lives. There exists an inherent human instinct to treat certain aspects of life as private, and this sense of privacy is closely linked to dignity, autonomy, and personal identity.[1]

Privacy, therefore, is not just a legal concept but also a lived human experience. It has often been described as the "right to be let alone," encompassing conditions such as solitude, intimacy, anonymity, and personal reserve. Adequate protection of privacy is essential for individuals to develop and preserve their identity, as well as to exercise their freedoms meaningfully.[2]

With globalization and rapid technological advancements, the collection and sharing of personal data have increased at an unprecedented pace. Public authorities, along with private entities, are now deeply involved in collecting and processing large volumes of data. This expansion has created new challenges in the field of data protection. The growing reliance on internet-based services and digital technologies has also increased the risk of data breaches, misuse, and unauthorized access. If not handled properly, personal data can become a highly sensitive and potentially harmful asset. The situation has become more complex in recent years, especially after the COVID-19 pandemic, which led to a sharp rise in digital transactions and online interactions, thereby intensifying concerns about privacy violations.[3]

In a democratic society, the ethical and lawful handling of data is crucial. A significant turning point in India came with the Supreme Court's decision in ***Justice K.S. Puttaswamy***

[1] Nuala O'Connor and Alethea Lange, et.al., Privacy in the Digital Age, Great Decisions 27 (Foreign Policy Association, 2015).
[2] Attila Peterfalvi, "Data Protection and Freedom of Information on Digital Platforms" 2021 (2) Law Review of Kyiv University of Law 348 (2021).
[3] EPW Engage, "What Enables the State to Disregard the Right to Privacy?" Economic and Political Weekly (Engage) 3 (2019), available at: https://www.epw.in/engage/article/what-enables-state-disregard-right (last visited on March 10, 2026)

***(Retd.)* v. *Union of India (2017)*[4],** which recognised the right to privacy as a fundamental right under Article 21 of the Constitution.[5] This landmark judgment laid the foundation for stronger data protection measures and highlighted the State's responsibility to protect individual freedoms. It also emphasized the need to regulate data collection and processing in a manner that allows individuals to retain control over their personal information.[6]

In response to these concerns, the Indian Parliament enacted the Digital Personal Data Protection Act, 2023 (DPDP Act). The primary objective of this legislation is to protect individuals' digital personal data and establish a structured framework for its lawful processing. The Act introduces a compliance mechanism, including penalties for violations and data breaches, thereby strengthening accountability.[7]

Before the enactment of this law, India did not have a comprehensive statute dedicated specifically to data protection. The existing framework relied largely on limited provisions under Sections 43A[8] and 72A[9] of the Information Technology Act, 2000, along with the Sensitive Personal Data or Information (SPDI) Rules, 2011. These provisions were inadequate to address the complexities of modern data processing practices carried out by both state and private actors.[10]

The need for a robust data protection regime was recognised by the Government of India through the appointment of the Justice B.N. Srikrishna Committee in 2017.[11] Based on its recommendations, the Personal Data Protection Bill, 2019 was introduced. After detailed examination by a Joint Parliamentary Committee, the bill was eventually withdrawn and replaced by a revised draft in 2022. The final version, the DPDP Act, 2023, was introduced and passed by Parliament in August 2023. Compared to the earlier bill, the Act adopts a simplified approach, though it draws inspiration from global frameworks such as the GDPR.[12]

---

[4] Justice K. S. Puttaswamy (retd.) v. Union Of India, (2017) 10 SCC 1.
[5] The Constitution of India, art. 21.
[6] Mohammad Omar Hashmi; Adnan Ahmad, "Data Protection Bill: A Comparative Study of the Indian Data Privacy Dilemma" 3(3) Jus Corpus Law Journal 515 (2023).
[7] The Digital Personal Data Protection Act, 2023, (Act 22 of 2023).
[8] The Information Technology Act, 2000, (Act 21 of 2000), s. 43A.
[9] *Id.* s. 72A
[10] Ministry of Communications and Information Technology, Department of Information Technology Notification, Dated April 11, 2011.
[11] Justice B.N. Srikrishna "A Free and Fair Digital Economy Protecting Privacy" Empowering Indians" Government of India (2017).
[12] Karishma Sundara and Nikhil Narendran, "Protecting Digital Personal Data in India in 2023 is the lite approach, the right approach?" 24 (1) Computer Law Review International Journal 9 (2023).

The DPDP Act establishes a legal structure governing the processing of digital personal data and defines the rights and responsibilities of individuals, referred to as "Data Principals." It grants individuals rights such as access to their data, correction, erasure, and the ability to nominate a representative. The Act emphasizes consent as the basis of data processing and seeks to promote transparency, accountability, and informational self-determination.[13]

At the same time, the Act attempts to balance privacy with other competing interests by allowing data processing for lawful purposes under a regulated framework. It aims to create a system that respects individual rights while also enabling legitimate data use. The law is expected to have a wide impact across various sectors, including legal services, information technology, human resources, finance, and marketing, as these sectors deal extensively with personal data. Organizations operating in these areas will be required to align their practices with the new legal framework.[14]

Importantly, the DPDP Act, 2023 also amends certain existing laws, including the Information Technology Act, 2000 and the Right to Information Act, 2005.[15] One of the most significant changes is the amendment to Section 8(1)(j) of the RTI Act[16] through Section 44(3)[17] of the DPDP Act. This amendment replaces the earlier provision concerning the disclosure of personal information.[18]

Under the amended provision, any information relating to personal data is exempt from disclosure under RTI requests. Previously, such information could still be disclosed if it satisfied the conditions of "public activity" or "larger public interest." However, the amendment removes these safeguards, effectively making privacy a stronger and, in many cases, overriding ground for non-disclosure.[19]

This change has attracted considerable criticism. Critics argue that the removal of the "public interest" test weakens the transparency framework established by the RTI Act. Even

[13] Angad Haksar, "Analysing the Digital Personal Data Protection Bill, 2022" 5 Indian Journal of Law and Legal Research 4 (2023).
[14] *Ibid.*
[15] The Right to Information Act, 2005, (Act 22 of 2005).
[16] *Id.* s. 8(1)(j).
[17] *Supra Note* 7. S. 44(3).
[18] Divyanshi Kaushal, "The Digital Personal Data Protection Bill, 2022" 3 (2) Jus Corpus Law Journal 748 (2022).
[19] Lalit Kalra, "Decoding the Digital Personal Data Protection Act, 2023", EY, August 23, 2023, available at: https://www.ey.com/en_in/cybersecurity/decoding-the-digital-personal-data-protection-act-2023 (last visited on March 10, 2026).

before the amendment, there were concerns that Public Information *Officers* frequently used the exemption clause to deny information. With the removal of qualifying conditions, the scope for such denials has increased further.[20]

As a result, public authorities may now refuse to disclose even those categories of personal information that would previously have been shared in the larger public interest. This creates a broad restriction on access to information and shifts the balance in favour of privacy. Additionally, the amendment grants greater discretionary power to Public Information Officers, increasing the possibility of subjective decision-making in the absence of clear guiding standards.[21]

2. Balancing Transparency and Privacy: The Relationship between RTI and the Right to Privacy

The right to freedom of speech and expression is a fundamental value recognised across the world, as it promotes individual development and self-fulfilment.[22] The right to information (RTI) emerges from this broader freedom and allows individuals to access information held by public authorities.[23] It empowers citizens to question the government, seek records, and remain informed about public affairs. In doing so, RTI plays a vital role in ensuring transparency and accountability in governance.[24]

In a modern democratic setup, particularly in the era of liberalisation and globalisation, the idea of a secretive government is no longer acceptable. Citizens, civil society organisations, consumers, and even businesses have a legitimate right to know how public authorities function, how decisions are made, and how public resources are used. The free flow of information strengthens democratic participation and builds trust between the government and the people.[25]

---

[20] Sivarama Krishnan and Anirban Sengupta, et.al., "The Digital Personal Data Protection Act, 2023" PWC.IN (2023)
[21] *Ibid.*
[22] *Supra Note* 5. Art. 19.
[23] Aparna Singh, "Right to Information Vis-A-Vis Privacy Right: Balancing of Interest" 7 RMLNLUJ 81 (2015).
[24] *Ibid.*
[25] The Right to Information, What is Right to Information, Wiki, available at: https://righttoinformation.wiki/guide/applicant/fundamental-facts-about rti#:~:text=RTI%20stands%20for%20Right%20to,and%20seek%20certified%20photocopies%20thereof. (last visited on March 10, 2026).

On the other hand, the right to privacy serves a different but equally important purpose. It protects an individual's personal space and safeguards them from unwarranted interference. Privacy allows individuals to control their personal information and prevents unnecessary intrusion into their private lives. In this sense, it acts as a limitation on the right to information, especially when the requested information relates to personal matters.[26]

Both the right to information and the right to privacy are essential human rights, and in many ways, they complement each other. While RTI facilitates access to information held by public authorities, privacy ensures that personal information is not disclosed without justification. The tension between the two arises when a request for information involves details that fall within an individual's private sphere.[27]

The concept of privacy has evolved over time. One of the earliest discussions on privacy can be traced back to the famous article by Samuel Warren and Louis Brandeis published in the *Harvard Law Review* in 1890. They described privacy as the "right to be let alone," highlighting the need to protect individuals from unwanted intrusion. Privacy was understood as the ability to enjoy one's personal life without interference and to control the disclosure of information related to oneself, including personal details and images.[28]

In legal terms, the right to information is often seen as a "positive right" because it enables individuals to actively seek and obtain information. Privacy, on the other hand, is generally regarded as a "negative right" because it protects individuals from intrusion into their life, liberty, and personal domain. However, modern legal developments have also recognised that privacy has a positive dimension, particularly in relation to protecting personal identity and dignity.[29]

Although these rights are interconnected, conflicts arise when transparency demands disclosure of information that may infringe upon an individual's privacy. In such situations, it becomes necessary to strike a careful balance between the two. This balance can only be

[26] Herbert Spencer Hadley, "Right to Privacy" 3(1) Northwestern Law Review 1 (1894).
[27] *Ibid.*
[28] *Ibid.*
[29] Vijay Pal Dalmia, "India: Data Protection Laws in India - Everything You Must Know" Mondaq, December 13, 2017, available at: https://www.mondaq.com/india/data-protection/655034/data-protection-laws-in-india---everything-you-must-know (last visited on March 10, 2026).

achieved through well-defined legal safeguards.[30]

Earlier, Section 8(1)(j) of the RTI Act attempted to maintain this balance by providing a qualified exemption for personal information. It allowed disclosure if the information was related to a public activity or if a larger public interest justified such disclosure. This approach ensured that neither transparency nor privacy was given absolute priority, and decisions could be made based on the circumstances of each case.[31]

Thus, the earlier framework under the RTI Act reflected an effort to harmonise the competing interests of access to information and protection of privacy. It recognised that while transparency is essential in a democracy, it should not come at the cost of unjustified intrusion into an individual's private life.[32]

3. Amendment to Section 8(1)(j) of the RTI Act, 2005 in Light of the DPDP Act, 2023 (Rewritten)

The primary objective of data protection laws is to establish clear rules for the collection and processing of data while ensuring that individuals' privacy is not unnecessarily intruded upon. In India,[33] the Digital Personal Data Protection Act, 2023 (DPDP Act) now serves as the main legislation governing the protection of digital personal data. The Act also has an extra-territorial reach, meaning it can apply to entities outside India if they deal with the personal data of individuals within the country.[34]

The DPDP Act has been designed to introduce changes to the existing legal framework without causing major disruption. At the same time, it aims to support initiatives such as ease of living, ease of doing business, and the growth of India's digital economy.[35]

Before the enactment of the DPDP Act, a balance between transparency and privacy was

[30] *Ibid.*
[31] *Supra Note* 16.
[32] *Supra Note* 15.
[33] Vijay Pal Dalmia, "India: Data Protection Laws in India - Everything You Must Know" Mondaq, December 13, 2017, available at: https://www.mondaq.com/india/data-protection/655034/data-protection-laws-in-india---everything-you-must-know (last visited on March 10, 2026).
[34] Kirk Naha and Roma Gujarathi, et.al., "India Passes Long Awaited Privacy Law", Wilmerhale Privacy and Cyber Security Law, August 18, 2023, available at: https://www.wilmerhale.com/en/insights/blogs/wilmerhaleprivacy-and-cybersecurity-law/20230818-india-passes-long-awaited-privacy-law (last visited on March 10, 2026).
[35] *Ibid.*

maintained under Section 8(1)(j) of the Right to Information Act, 2005. This provision allowed public authorities to withhold personal information, but only under certain conditions. Importantly, it included safeguards such as the "public interest" and "public activity" tests. These conditions ensured that personal information could still be disclosed if it served a larger public interest, thereby maintaining a balance between an individual's privacy and the public's right to know.[36]

However, the DPDP Act, through Section 44(3), has amended Section 8(1)(j) of the RTI Act. The revised provision significantly changes the earlier position by broadly exempting all personal information from disclosure under RTI. The language of the amendment suggests that any information classified as "personal" can be denied without considering whether its disclosure would serve a public purpose.[37]

This shift has attracted considerable criticism. The earlier provision was carefully structured to balance competing interests, whereas the amended version appears to tilt heavily in favour of privacy. By removing the conditions related to public interest and public activity, the amendment effectively converts a qualified exemption into a blanket exemption.[38]

As a result, Public Information Officers (PIOs) now have greater discretion to deny access to information. They are no longer required to assess whether the disclosure of personal information is justified in the larger public interest. This change risks undermining the core objective of the RTI Act, which is to promote transparency and accountability in governance.[39]

The government has defended this amendment by stating that it seeks to harmonise the RTI framework with modern data protection principles. However, critics argue that such harmonisation should not come at the cost of weakening the right to information.[40]

Under the original Section 8(1)(j), personal information could be withheld only if it had no connection to public activity or if its disclosure would lead to an unwarranted invasion of

[36] *Supra Note* 16.
[37] *Ibid.*
[38] *Ibid.*
[39] Ministry of Electronics and IT, "Salient Features of the Digital Personal Data Protection Bill, 2023" Press Information Bureau, August 09, 2023, available at: https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1947264 (last visited on March 10, 2026).
[40] *Ibid.*

privacy. Even then, disclosure was permitted if a larger public interest justified it. This framework ensured that transparency was not sacrificed entirely in the name of privacy.[41]

Judicial interpretation in India has also supported this balanced approach. Courts have consistently held that personal information may be disclosed if it serves a public interest and does not unjustifiably violate privacy. At the same time, they have protected genuinely private information from disclosure, especially in cases involving sensitive personal details.[42]

The 2023 amendment, however, changes this settled position. Now, even if the requested information is linked to public interest, authorities are not legally bound to disclose it if it falls under the category of personal information. This creates a broad restriction on access to information and increases the likelihood of rejection of RTI applications.[43]

Another major concern is the absence of a clear definition of "personal information" in the DPDP Act. This lack of clarity gives wide discretionary power to authorities, allowing them to interpret the term broadly. As a result, even information related to public records or policy matters may be denied on the ground that it contains personal details.[44]

Further, the scope of the term "person" under the DPDP Act is quite wide and includes individuals, companies, associations, and even the State. This raises concerns that information relating to various entities could also be withheld under the guise of protecting personal information.[45]

The amendment may also have far-reaching consequences for transparency in welfare schemes and public administration. For example, access to information about beneficiaries of government schemes, such as ration distribution, pensions, or scholarships, is crucial for ensuring accountability and preventing corruption. If such information is denied on privacy grounds, it may weaken mechanisms like social audits and public oversight.[46]

---

[41] *Supra Note* 16.
[42] *R.K Jain* v. *Union of India,* (2013) 14 SCC 794.
[43] Shailesh Ghandi, "How the proposed Data Protection Bill will undermine India's Right to Information" Scroll.in, November 21, 2023, available at:https://scroll.in/article/1037879/how-the-proposed-data-protectionbill-will-undermine-indias-right-to-information (last visited on March 10, 2026).
[44] *Ibid.*
[45] *Ibid.*
[46] *Ibid.*

In practice, the RTI regime in India has played an important role in promoting transparency over the past two decades. Many RTI applications have sought detailed information, including names, addresses, and records, which were earlier disclosed when justified by public interest. With the new amendment, there is a growing concern that such disclosures may now be routinely denied.[47]

The DPDP Act emphasizes the role of consent in data processing and introduces safeguards such as lawful, specific, and informed consent of the data principal. While these principles are important for protecting privacy, their application in the context of RTI must be carefully balanced to ensure that transparency is not compromised.[48]

The Supreme Court has also laid down the principles of legality, necessity, and proportionality in matters relating to privacy. Any restriction on access to information must therefore meet these standards. The earlier version of Section 8(1)(j) aligned with this approach by allowing a case-by-case assessment. However, the amended provision appears to move away from this balanced framework.[49]

Thus, the amendment introduced by the DPDP Act, 2023 marks a significant shift in the relationship between privacy and transparency in India. By turning a conditional exemption into a broad and largely absolute one, it raises serious concerns about its impact on the effectiveness of the RTI Act. The delicate balance that once existed between the right to information and the right to privacy now appears to be under strain.[50]

4. Impact of the GDPR on the Freedom of Information Act, 2000 in the United Kingdom

The General Data Protection Regulation (GDPR),[51] which came into force on 25 May 2018, was introduced to establish a uniform framework for data protection across the European Union. It replaced the earlier Data Protection Directive of 1995 and aimed to strengthen privacy rights while ensuring consistency in data protection standards among EU member states.[52] At

[47] The Hindu Bureau, "Digital Personal Data Protection Bill, 2023 passes in Lok Sabha; govt. shrugs off exemptions" The Hindu, August 07, 2023, available at: https://www.thehindu.com/news/national/data-billpasses-in-lok-sabha-govt-shrugs-off-exemptions/article67167943.ece (last visited on March 10, 2026).
[48] *Ibid.*
[49] *Supra Note* 16.
[50] *Ibid.*
[51] The General Data Protection Regulation, 2018, (EU 679 of 2016).
[52] Lothar Determann; Chetan Gupta, "India's Personal Data Protection Act, 2018: Comparison with the General

the same time, it allowed individual countries to introduce additional safeguards where necessary. Privacy has long been treated as a fundamental right within the European framework, and the GDPR reflects this strong commitment.[53]

The GDPR focuses on protecting personal data and lays down detailed rules for how such data should be collected, processed, and stored. It also provides individuals, referred to as "data subjects," with a range of rights over their personal information.[54] These include the right to access, correct, and control the use of their data. A key feature of the GDPR is its emphasis on consent and lawful processing, ensuring that personal data cannot be used arbitrarily.[55]

In the United Kingdom, the Freedom of Information Act, 2000[56] (FOI Act) serves a different but equally important purpose. It enables individuals to access information held by public authorities, thereby promoting transparency and accountability in governance. While the GDPR focuses on protecting personal data, the FOI Act facilitates the disclosure of information in the public interest.[57]

The interaction between these two laws becomes important when an FOI request involves personal data. In such cases, authorities must carefully balance the need for transparency with the obligation to protect individual privacy. This creates a point of intersection where both legal frameworks must be applied together.

Section 40 of the FOI Act, 2000 deals specifically with exemptions related to personal data. It provides that personal information may be withheld from disclosure under certain conditions. Following the implementation of the GDPR, changes were made to how this provision is interpreted and applied.[58] In particular, Section 40(8) now requires that decisions regarding disclosure be assessed in light of the GDPR's standards, especially those relating to lawful

Data Protection Regulation and the California Consumer Privacy Act of 2018" 37(3) Berkeley Journal of International Law 504 (2019).

[53] Steven M. Puiszis, "Unlocking the EU General Data Protection Regulation" 2018 Journal of the Professional Lawyer 2 (2018).

[54] W. Gregory Voss, "European Union Data Privacy Law Reform: General Data Protection Regulation, Privacy Shield, and the Right to Delisting" 72 (1) The Business Lawyer 222 (2017).

[55] Brian Daigle and Mahnaz Khan, "The EU General Data Protection Regulation: An Analysis of Enforcement Trends by EU Data Protection Authorities" Journal of International Commerce & Economics 2 (2020).

[56] Freedom of Information Act, 2000, (United Kingdom, Chapter 36 of 2000).

[57] Nidirect, Freedom of Information and Data Protection, available at: https://www.nidirect.gov.uk/articles/freedom-information-and-data-protection (last visited on March 10, 2026).

[58] *Supra Note* 56. A. 40.

processing.[59]

One of the most relevant principles in this context is the first data protection principle under the GDPR, which requires that any processing of personal data must be lawful, fair, and transparent. This means that when a public authority receives an FOI request involving personal data, it must determine whether disclosing that data would meet these requirements. If disclosure is considered unfair, unlawful, or disproportionate, the information can be withheld.[60]

It is important to note that Section 40(1) of the FOI Act remains largely unaffected by the GDPR, as it relates to requests made by individuals for their own data. Such requests are treated as subject access requests under data protection law.[61] However, Sections 40(2)[62] and 40(3A),[63] which deal with third-party personal data, have been significantly influenced by GDPR principles.[64]

Before the GDPR came into force, public authorities relied on the Data Protection Act 1998, particularly Schedule 2, to determine whether the disclosure of personal data was justified. This often involved assessing whether disclosure served a "legitimate interest." With the introduction of the GDPR, this framework has been replaced by Article 6, which outlines the lawful bases for processing personal data, including legitimate interests.[65]

Under the GDPR, public authorities generally cannot rely on "legitimate interests" as a basis for processing personal data when performing their official functions. However, in the context of FOI requests, this ground can still be considered when determining whether disclosure is justified. This is because Section 40(8) of the FOI Act allows authorities to assess whether disclosure would comply with the GDPR's lawfulness requirement.[66]

As a result, a more structured and balanced approach has emerged. Public authorities must now evaluate whether disclosure of personal data under an FOI request is necessary, fair, and

[59] *Id.* s. 40(8).
[60] *Ibid.*
[61] *Supra Note* 56. S. 40(1).
[62] *Id.* s. 40(2).
[63] *Id.* s. 40(3A).
[64] *Ibid.*
[65] Capsticks, Revised section 40 of the Freedom of Information Act, available at: https://www.capsticks.com/insights/revised-section-40-of-the-freedom-of-information-act (last visited on March 10, 2026).
[66] *Ibid.*

proportionate. This ensures that privacy is not compromised unnecessarily, while still allowing access to information where justified.[67]

Therefore, the introduction of the GDPR has significantly influenced the operation of the FOI Act in the United Kingdom. Rather than completely restricting access to information, it has reshaped the decision-making process by embedding stronger data protection standards. The current framework attempts to maintain a balance between transparency and privacy, ensuring that both rights are respected without giving absolute priority to either.[68]

5. Conclusion

The rights to information and privacy are both essential for protecting the dignity and autonomy of individuals. These rights share a complex relationship at times, they support each other, while at other times they come into conflict. In today's digital world, where technology and internet use have become an integral part of daily life, the collection and processing of data have increased significantly. Personal data is no longer just information; it has become a valuable asset that requires strong protection against misuse and unauthorised access.[69]

For a long time, India lacked a comprehensive legal framework specifically dedicated to data protection. Existing laws were limited in scope and often insufficient to address the challenges posed by modern data practices. The recognition of the right to privacy as a fundamental right marked a turning point and strengthened the demand for a robust data protection regime. This eventually led to the enactment of the Digital Personal Data Protection Act, 2023, which seeks to regulate the processing of digital personal data while protecting individual rights.[70]

The DPDP Act introduces an important framework based on consent, accountability, and transparency. It reflects global trends, particularly those seen in the GDPR, by recognising the principle of informational self-determination and giving individuals greater control over their personal data. At the same time, the Act attempts to balance individual rights with the legitimate

[67] Information Commissioner, Personal information (section 40 and regulation 13), available at: https://ico.org.uk/for-organisations/foi/section-40-and-regulation-13-personal-information/ (last visited on March 10, 2026).
[68] *Ibid.*
[69] *Ibid.*
[70] *Supra Note* 7.

needs of data processing in a modern economy.

However, one of the most debated aspects of the Act is its amendment to Section 8(1)(j) of the Right to Information Act, 2005. The RTI Act has long been a key tool for ensuring transparency and accountability in governance. Earlier, it maintained a balance between privacy and access to information by allowing disclosure of personal information where it served a larger public interest or was related to a public activity. The removal of these conditions has significantly altered this balance.

The amended provision now treats personal information as broadly exempt from disclosure, without requiring a consideration of public interest. This raises concerns that the transparency-promoting function of the RTI Act may be weakened. The absence of clear distinctions between purely private information and information linked to public accountability further adds to the ambiguity.

A comparative perspective from the United Kingdom highlights a different approach. While the introduction of the GDPR also influenced the Freedom of Information Act, 2000, it did not completely override access to information. Instead, it introduced structured safeguards such as fairness, lawfulness, and proportionality, along with the concept of legitimate interest. This approach attempts to balance privacy and transparency rather than giving absolute priority to either.

Before the 2023 amendment, Section 8(1)(j) of the RTI Act similarly reflected a balanced approach in India. It recognised that privacy is not an absolute right and must be harmonised with other fundamental rights, including the right to information. The recent changes, however, appear to shift this balance more strongly in favour of privacy, raising important questions about their long-term impact on transparency and democratic accountability.

Ultimately, both privacy and access to information are vital in a democratic society. Neither right should be allowed to override the other completely. While personal information must be protected from unjustified intrusion, transparency must not be sacrificed under the broad claim of privacy. The responsibility lies with the State to ensure that these rights are balanced carefully and applied in a manner that promotes both individual freedom and public accountability.