The Dialogue™
INFORM ENGAGE IDEATE

Policy Brief September, 2022

NAVIGATING THE FUNDAMENTAL RIGHT TO PRIVACY IN INDIA

Authors : Bhavya Birla and Garima Saxena

Table of Content

Introduction

The ruling of the Supreme Court in the ***Justice K.S. Puttaswamy v. Union of India & Ors I***[1] represents a crucial development in the privacy jurisprudence in India. The much-celebrated judgement by a nine-judge bench revisited the question of whether the right to privacy was guaranteed by our Constitution and upheld privacy as a fundamental right protected under Article 21. Although privacy has been previously granted the status of a constitutional right in some or other form in several judgments, the Puttaswamy ruling resolved a *"generational question"* and introduced a possibility of an era of Constitution 3.0.[2] The judgement, while carefully scrutinising the Aadhaar project and the constitutional validity of the Aadhaar Act, 2016, elaborated on the right to privacy and allied issues, ranging from informational privacy, decisional autonomy, surveillance and data protection. It also discussed the necessity and significance of a data protection framework and highlighted the data protection principles such as consent, collection limitation, purpose limitation, access, erasure, etc.

More essentially, the judgement laid down a precedent for itself and other courts to follow while deciding upon matters related to violation of privacy and allied rights. Resultantly, the Supreme Court and several high courts have heavily relied on Puttaswamy to nurture jurisprudence with respect to the right to privacy. This has not only acted as a means for individuals to access their rights but has also laid down an approach that the government might take into consideration and rely on while drafting the new data protection legislation.

For the purposes of this brief, we have chosen principles on the basis of jurisprudential development in India. We have narrowed our approach to focus on these principles to assess the judiciary's acceptance and subsequent nurturing of data subject rights in a legislative vacuum. Such an assessment, we believe will assist us in understanding how the judiuciary will navigate on principles when a comprehensive data regulatory framework is eventually implemented. Therefore, it is essential to trace how certain principles have been interpreted and applied by the courts in several cases. We also explore recommendations based on the Puttaswamy mandate and the global best practices.

Data Subject Rights

Data subject rights are accorded to individuals whose data is collected and processed by data processors and fiuciaries. These rights exist to balance the historically tilted data collection and processing processes where data companies were very lightly regulated and had plenty leeway to transfer and process personal data without limitation. As a measure to balance the scale, data subjects are given powers to ensure that companies do not breach limitations imposed on them through data regulations.

---

[1] *Justice K.S. Puttaswamy v. Union of India & Ors* I (Supreme Court of India) (2017) 10 SCC 1

[2] Atrey,S. & Bhatia, G. (2021 April) *New Beginnings: Indian Rights Jurisprudence After Puttaswamy*, University of Oxford Human Rights Hub Journal Vol 3(2). Retrieved on August 22, 2022 from https://ohrh.law.ox.ac.uk/wp-content/uploads/2021/04/U-of-OxHRH-J-New-Beginnings-2-1.pdf

Right to Know and Access Information

In India, the right to information flows from the fundamental right to speech and expression under Article 19(1)(a) of the Constitution and has been institutionalised as the Right to Information Act, 2005 ("RTI Act") and has been evolving since. The right to know and access information has been recognised as a fundamental right and an essential principle in promoting good governance. However, the principle has been assessed and developed by the courts in light of an individual's access to another individual's personal data as well and has provided a broader interpretation to the application of the Act. If a similar approach is applied to an individual's right to access their personal information, it would lead to increased transparency in terms of information available with the data fiduciary and enable the data principals to exercise the allied rights, including the right to erasure and right to portability.

There is, however, a need to firstly differentiate between it and the impugned principle of the right to know and access information as they both complement one another but do entail different connotations for the data subject. The right to know and access information is available for data subjects to seek information about who has their personal data, what processing has been undertaken on it and to whom the data was transferred and why. This principle is present to ensure that the data subject is aware of where their data currently resides and to assess whether data processing is within the ambit of the reasons the data was collected in the first place.

As also recognised in the B.N. Srikrishna report titled "A Free and Fair Digital Economy Protecting Privacy, Empowering Indians",[3] the principle is particularly significant "in situations where the proliferation of actors and the technological complexity of practice make it difficult for the data subject to know and understand whether, by whom and for what purpose personal data relating to him or her are being collected, such as in the case of online advertising."[4] Clause 17 of the erstwhile Personal Data Protection Bill 2019 provided the data principals with the right to obtain confirmation about the processing of data, details of the personal data processed or being processed, and supplementary information related to processing activities undertaken with respect to the personal data. The Joint Parliamentary Committee (JPC) on the PDP Bill 2019 had also observed the need for the inclusion of the right for data principals to nominate legal heirs to exercise specific rights on behalf of data principals upon their death. The right plays a vital role in furthering transparency and accountability in activities related to the processing of personal data of the data principals and also allows them to exercise allied rights such as the right to erasure and the right to correction. While the bill is yet to concretise these rights on us, they have been put to the test in various cases.

For instance, in 2020, the Central Information Commission in ***Saurav Das vs Dept. Of Information***

[3] Committee of Experts under the Chairmanship of Justice B.N. Srikrishna (2018, July 27) *A Free and Fair Digital Economy*: *Protecting Privacy, Empowering Indians*, Ministry of Electronics and Information Technology. Retrieved on August 22, 2022 from https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf

[4] Recital 58, General Data Protection Regulation, 2018. Retrieved on August 21, 2022 from https://www.privacy-regulation.eu/en/recital-58-GDPR.htm

Technology[5], the complainant sought details about the development and legality of Aarogya Setu through the provisions of the RTI Act from the CPIO, National E-Governance Division, MeitY and CPIO, MeitY. Given the urgency and sensitivity of the matter, the Commission provided an early hearing opportunity to the complainant. Amongst other significant observations, the Commission acknowledged the principles of data protection that were given recognition in the design and implementation of the Aarogya Setu app such as consent, purpose limitation, data retention, users' rights, etc. It also issued an advisory under Section 25(5) of the RTI Act, 2005 to the Secretary, MeitY to make sure that the Aarogya Setu website was robust and updated so as to enable citizens to access information on the subject without resorting to the RTI.

In the case of ***Central Public Information Officer, Supreme Court v. Subhash Chandra Agarwal***[6], wherein the Hon'ble Court held that the office of the Chief Justice of India constitutes a public authority under Section 2(h) of the RTI Act, 2005. It was observed by the Court that the RTI regime ensures a balance between the right to know and the right to privacy through Sections 8(1)(j) and 11 and by applying the larger public interest test. The three-pronged test of proportionality developed in the Puttaswamy judgement, assessing the necessity and legality of policy decisions, was also used to examine the validity of the intrusions under the RTI law, and it was held that the provisions fulfilled the criteria.

Recommendation: While the jurisprudence around the right to know and access information as a data protection principle has not witnessed much development, the right to access public information has received a much broader interpretation and application. The right to privacy and the right to access information may be conflicting at times, but they work together to enhance transparency and accountability in processes. It, therefore, becomes essential that the new data protection framework aims to harmonise the two rights and ensure that the data protection legislation is in line with the the core norms of the RTI Act while conforming with the privacy principles laid out in the Puttaswamy judgment.

Data Minimisation

The principle of data minimisation recognises the need to collect only such data that it is necessary to serve the purpose – for which it was collected. The Apex Court, while examining the provisions of the Aadhaar Act, 2016[7] in the Puttaswamy judgment, concluded that the Aadhaar project was in alignment with the principle of data minimisation as Section 2(k) of the 2016 Act put a restriction on the collection of sensitive information such as race, religion, caste, tribe, ethnicity, language, records of entitlement, income or medical history. Moreover, the Unique Identification Authority of India (UIDAI) is also restricted from collecting, storing or maintaining, either directly or indirectly any information about the purpose of authentication, thereby recognising the principle of data minimisation. The principle had also been recognised under Clause 6 of the erstwhile PDP Bill, 2019 which mandated the collection of data only to the extent necessary for the purposes

[5] *Saurav Das v. Dept. Of Information Technology*, (Centeral Information Commission) CIC/DEOIT/C/2020/685084.
[6] *Central Public Information Officer, Supreme Court v. Subhash Chandra Agarwal*, (Supreme Court of India) 2019 SCC OnLine SC 1459.
[7] The Aadhaar (Targeted Delivery Of Financial And Other Subsidies, Benefits And Services) Act, 2016 (2016 March 26) Unique Identification Authority of India.

of processing such personal data. While the PDP Bill 2019 was withdrawn recently, still data minimisation principle was tested in the court under following cases.

The Kerala High Court in ***Ramesh Chennithala v. State Of Kerala***[8] dealt with a Public Interest Litigation (PIL) challenging the circular issued by the State Police Chief to the Additional Director General Police and Police Head Quarters to take up the matter with BSNL, VODAFONE and ensure collection of Call Data Records (CDRs) of COVID-19 positive patients. The Court was informed by the respondents that such data was collected 14 days before the patients become positive. While recognising the data protection principles such as confidentiality of the CDR details collected, restriction on third party access, and limitation on use of data for any other purpose, the Court did not grant the petitioner the permission to implead the service providers to decide whether the data provided by the service providers can be limited to the information about the tower location.

In 2021, the Karnataka High Court in ***Anivar A Aravind v. Ministry of Home Affairs***[9] passed an interim order prohibiting the central government and National Informatics Centre (NIC) from sharing the health data of citizens without their informed consent. The Court, while scrutinising the privacy policy of Aarogya Setu in light of the principle of notice, observed that the app allowed an individual to download his personal data only after the Terms of Service and Privacy Policy of the app was brought to his notice and the fact that his mobile number was essential for contact tracing. It was also highlighted that an individual was provided with adequate notice regarding the use of data for specific purposes, data transfer, retention, etc. While the Court did not specifically touch upon the principle of data minimisation, it did recognise the need to collect data for limited and specific purposes.

Similarly, the Supreme Court of India in the case of ***Manohar Lal v. Union of India***[10] elaborated upon the right to privacy in the information age and upheld privacy to be a "sacrosanct" right in consonance with the Puttaswamy judgment. In the instant case, the Supreme Court elaborated upon the trade-off between the right to privacy of the individuals and the security interests of the State and realised the need to appoint an Expert Committee to look into the allegations made in the Pegasus spyware case. The Court ruled that unauthorized surveillance or accessing of stored data from the phones and other devices of citizens for reasons other than the nation's security would be illegal, objectionable and a matter of concern.

Earlier, in 2020, the Central Information Commission in ***Saurav Das vs Dept. Of Information Technology***[11] had also recognised the principles of data protection that were given recognition in the design and implementation of the Aarogya Setu app such as consent, purpose limitation, data retention, users' rights, etc.

[8] R*amesh Chennithala v. State Of Kerala*, (Kerela High Court) WP(C).No.17028 OF 2020.
[9] *Anivar A Aravind v. Ministry of Home Affairs*, (Karnataka High Court) WP No. 7483 of 2020.
[10] *Manohar Lal v. Union of India*, (Supreme Court of India) Writ petition (criminal) No.314 of 2021.
[11] *Saurav Das v. Dept. Of Information Technology* (Central Information Commission) CIC/DEOIT/C/2020/685084.

Recommendation: Data minimisation must be implemented in the manner pronounced by the Puttaswamy judgement. Collection and storage of data must be based on minimised principles in order to ensure that individual privacy is not impinged on. Purpose limitation which was upheld in the puttaswamy judgement, and across multiple sections of the erstwhile PDP Bill, 2019 need to be factored in by the judiciary and the legislature to ensure that data protection is safeguarded against abuse.

Data Retention

The principle of data retention recognises the need to retain or store information only until it serves the required purpose. It has been acknowledged as a necessary component of data protection laws and is found across GDPR, CCPA and in previous versions of India's data protection bill. Clause 9 of the erstwhile 2019 Bill obligated data fiduciaries to not to retain any personal data of the data principals beyond the required period and necessary purposes. The principle of data retention has been carried forward and granted unique interpretations by courts across the country as follows.

In the case of ***Balu Gopal Krishnan v. State of Kerala***[12], the Kerala High Court dealt with the concerns around data anonymisation and transfer of sensitive health data of COVID-19 patients outside India. In 2020, the Kerala Government entered into a contract with Sprinklr Inc., a U.S.-based IT firm, to collect, manage and analyse the health data of COVID-19 patients in Kerala. As the Kerala Government was not equipped with the resources to manage such large quantities of data, it engaged the U.S. company to carry out effective management of the pandemic in the state. The judgement reflects a novel stance of the judiciary in dealing with and maintaining a balance between public health crises and the right to privacy of individuals. While the Court restricted itself from examining the various allegations put forth by the petitioners, it issued guidelines as an interim measure to prevent the breach of confidentiality of the data collected by the State and processed by Sprinklr and to ensure that there was no "data epidemic"[13] after the COVID-19 pandemic. The Court directed the state government to anonymise the data collected with Sprinklr and inform citizens about such data being accessible to third parties to take specific consent from the citizens. The company was also injuncted from breaching the confidentiality of the data and advertising or representing that they are in possession of such data and deriving any commercial benefits out of such data. More importantly, while the judgment did not restrict the state government from engaging the services of the company, it directed Sprinklr Inc. to entrust all the data back to the state government in the future after the processing has been done and also entrust back any or secondary data available to the government.

Recommendation: Government initiatives must respect the bounds laid down by the two Puttaswamy judgements in order to be in compliance with the legal norms up until a data protection framework is brought out. Any data initiatives that the government proposes to bring in the interim must ensure that data retention norms are in line with prudent purpose

[12] *Balu Gopal Krishnan v. State of Kerala* (Kerala High Court) W.P. (C), Temp No. 84 of 2020.
[13] Refers to the misuse and abuse of data collected by public and private authorities during the pandemic, especially without a legislative backing.

limitations. The Puttaswamy mandate however has not been followed in the recent CERT-IN guidelines for VPN service providers that mandated 'Identified Entities' to maintain logs of ICT systems for a rolling period of 180 days and data centres, VPS, cloud service providers and VPN providers to retain the listed meta data including names, emails and IP addresses, ownership patterns and purpose for hiring services, for 5 years or more, etc.[14] Such arbitrary data retention mandates are disproportionate for the goal they wish to achieve and need to be brought within the ambit of the Puttaswamy mandate.

Informational Privacy

In a data-fied world that is moving rapidly towards digitisation, the ability of a data subject to be protected against disproportionate and intrusive collection of their data form the basis of the need for informational privacy. The principle, while accepting the power of data points on revealing our intimate details and its aggregation as a means to profile, have long been central in the fight for privacy against using data as a means to surveil.

The concept was dealt with at length in the Puttaswamy case where the court discussed the very nature of 'information' as nonrivalrous, invisible and recombinant in its use while establishing that mining of such data without oversight would constitute surveillance. The apex court in furthering its position as a protector against unwarranted data mining, held that publishing voter data in searchable format would allow for private mining of data and voter profiling in the case of ***Kamal Nath v. Election Commission of India & Ors***[15] and ruled against providing the same in a searchable format to the petitioner. The court furthered its role of a protector of informational privacy in cases where personal dignity was involved, ruling for a balance between the privacy of the victim and the right to a fair trial of the accused in the case of ***P . Gopalkrishnan vs. State of Kerala and Ors***[16] where the court balanced the right of the victim to not be subject to violation of their privacy by making a video of their rape as a documentary evidence and the accused's right to know the veracity of the evidence posited against them.

Similarly in the case of ***Ananga Kumar Otta v. Union of India & Ors***[17] the court ruled that disclosure of names of persons with COVID-19 (whether in self isolation or quarantined in private or state hospitals) needed to be curtailed in order to stop the violation of their privacy after private citizens began proliferating personal details of such persons on social media. The court assessed the social stigma that was resultant of such disclosures and asked the government of Orissa to cease such disclosures and to anonymise personal information of persons when such disclosures are needed for internal purposes or case reporting.

Recommendations: It is evident that informational privacy can only be protected adequately when the government acts on its positive responsibility to bring forth a comprehensive data protection framework. In the interim, we recommend that users use privacy tools and take

[14] Indian Computer Emergency Response Team (CERT-In) (2022, April 28)*Cybersecurity Directions*, Ministry of Electronics and Information Technology. Retrieved on August 22, 2022 from https://www.cert-in.org. in/PDF/CERT-In_Directions_70B_28.04.2022.pdf
[15] *Kamal Nath v. Election Commission of India & Ors* (Supreme Court of India) 2019 2 SCC 260
[16] *P . Gopalkrishnan vs. State of Kerala and Ors* (Supreme Court of India) AIR 2020 SC 1
[17] *Ananga Kumar Otta v. Union of India & Ors.* (High Court of Orissa) Writ Petition (PIL) No.12430 of 2020

their online privacy into their hands. It can begin with us being mindful of sharing our personal information such as phone numbers or addresses with vendors or individuals in situations we don't deem so prudent. It can also be achieved by ensuring that websites we visit are encrypted and the platforms we use to voice ourselves or interact with one another are end-to-end encrypted to ensure our informational privacy is intact. These measures protect our informational privacy in the interim and complement the protections that will be accorded to us under a comprehensive data protection framework.

Anonymisation

Anonymisaton refers to the process of removing data points from data seta that can allow one to identify the person from who the data was collected. Anonymisation or 'de-personalising' data is an integral principle of data privacy as it presents at least in theory, a mid-path where companies aren't deprived of data for drawing insights and neither is the individual's privacy jeopardised in the process. However, true anonymisation is often regarded as 'unachievable' as data sets can be aggregated in order to find persons involved and has been found to be a hindrance in the application of anonymisation principles.[18] In the case of ***Balu Gopalakrishnan v. State of Kerala and Ors***[19], the Kerela High court adjudged the transfer of sensitive health data during the pandemic and ordered the state government to anonymise data sets before sharing them with the contracted party. The court had to intervene in this manner after holding the contract in place between the Kerela government and 'Sprinklr Inc.' (the contracted company) as insufficient in safeguarding individual privacy.

The central government has taken the principle forward by including it in the Non-Personal Data Framework that criminalises any effort to re-identify anonymised data sets in order to add a layer of protection for individual privacy.

Recommendation: The lack of clear dichotomies between definitions of personal and non-personal data present significant regulatory challenges. As a result, while the move to criminalise re-identification of data is a step in the right direction, it is merely the first prong of an effective regulatory framework. Issues with regulatory overlaps between personal and non-personal data where multiple regulators intersect, need to be harmonised by the Data Protection Authority for effective regulation. For instance, interlinkage of non-personal data (anonymised) set can reveal the personal identity of the individuals due to triangulation and also cause collective privacy harms which needs to be appropriately tackled. Furthermore, a lack of a clear definition coupled with a lack of anonymisation standards, shifts responsibility upon data processors to decide whether the data they share after processing is anonymised enough which has ramifications for the individual as well as the society as a whole considering the volume of data sets that are transferred in the data market.

[18] Rocher,L. Et al (2019 July 23) Estimating the *success of re-identifications in incomplete datasets using generative model*, Nature Communications. Retrieved from https://www.nature.com/articles/s41467-019-10933-3

[19] *Balu Gopalakrishnan v. State of Kerala and Ors* (Kerela High Court) W.P. (C). Temp No. 84 of 2020 along with other petitions

[20] Internet Freedom Foundation (2020, June 30) *MoRTH scraps its Bulk Data Sharing Policy but THIS IS NOT IT!* Retrieved on August 17, 2022, from https://internetfreedom.in/morth-bulk-data-sharing-policy-scrapped/

[21] Joshi, D. (2020, July 30). *Non-Personal Data Regulation: Interrogating 'Group Privacy'*. Centre for Law & Policy Research. Retrieved on August 17, 2022, from https://clpr.org.in/blog/non-personal-data-regulation-interrogating-group-privacy/

Consent

Consent formulates the foundation for individual privacy in a digitalised world. Globally and domestically, data protection laws allow for the processing, collection and transfer of data only after the data subject consents to the same. It was present under clause 11 of the erstwhile PDP Bill and it was a necessary precursor before data processors can process personal data. However, multiple experts including the Justice B.N. Srikrishna Committee[22] had gone on record to state that consent in the manner that it is was proposed under the erstwhile PDP Bill, 2019 would lead to 'consent fatigue' a situation where the data subject is overwhelmed by the magnitude of consent requests to the point where informed consent cannot be provided as the data subject no longer understands what they are consenting to.

The apex court in ***Joseph Shine v. Union of India***[23], while reading down the punishment for Adultery as provided under section 497 of the Indian Penal Code (IPC), held that the consent of a woman and her right to privacy in choosing her partners was significantly undermined by an archaic provision in law (namely section 497 of the IPC and section 198(2) of the Criminal Procedure Code) and needed to be read down in light of the puttaswamy judgement's reiteration of privacy including the right to protect one's own sexual autonomy. Similarly, the definition of 'unnatural' under section 377 of the IPC was read down in the case of ***Navtej Singh Johar& Ors. v. Union of India***[24] as the impugned provision restricted an individuals right to exercise their bodily autonomy and their right to indulge in sexual activities in same-sex relationships with consenting adults.

Recommendation: The principle of consent is integral to a representative and inclusive data protection policy. However, consent fatigue is a real consequence that the government must accept as such and work towards minimising. The Consent dashboard model espoused by the Justice B.N. Srikrishna committee can be incorporated in order to reduce consent fatigue.

Dark patterns in terms of designing services also need to be factored in at a legislative level. While there has been plenty emphasis on the need for Privacy by Design (PbD), addressing dark patterns and their impact on informed consent is often underlooked. Dark patterns are the technological design choices made by businesses, which trick the users into acting in a particular manner while not intentionally choosing that behavior or action.[25] In the case of consent managers, a dark pattern could manifest in design choices that make accessing the details of our consent harder to access such as a separate page that requires the user to click and navigate to fullly assess what they're consenting to. Such dark patterns affect informed consent by playing human cognition and our general tendency to take the path of least

[22] Committee of Experts under the Chairmanship of Justice B.N. Srikrishna (2018, July 27) *A Free and Fair Digital Economy*: Protecting Privacy, Empowering Indians, Ministry of Electronics and Information Technology. Retrieved on August 21, 2022 from https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf

[23] *Joseph Shine v. Union of India* (Supreme Court of India) (2019) 3 SCC 39

[24] *Navtej Singh Johar& Ors. v. Union of India* (Supreme Court of India) (2018) 10 SCC 1

[25] United States Federal Trade Commission (n.d.) Dark Patterns Workshop Transcript. Retrieved on August 22, 2022 from https://www.ftc.gov/system/files/documents/public_events/1586943/ftc_darkpatterns_workshop_transcript.pdf

resistance, especially when the repercussions are not tangible and felt immediately.[26] Therefore interaction of dark pattern with consent management must be tackled effectively.

Right to be forgotten (De-linking/De-referencing)

The right to be forgotten is a data subject's right to contest the relevance or necessity of information about them online and the subsequent removal of the same when ruled irrelevant, unnecessary and not serving any legitimate interest. It was present under clause 20 of the erstwhile Data protection Bill (DPB) and had been stated to be present in the comprehensive bill to be tabled in an affidavit filed by the central government at the Delhi High Court. Whether the same still stands is yet to be seen since the recall of the erstwhile Data Protection Bill, 2021.[27]

The principle allows for people to contest the removal of information about them that can be damaging to their reputation and no longer represents their current reputation. While the right has long been adjudicated upon by foreign courts such as the Court of Justice of the European Union (CJEU) where the principle first arose when one, Mario Costeja Gonzalez contested the removal of an auction notice from Google Spain as the webpage caused inaccuracies in his finances. The court, while directing Google Spain to remove the impugned notice, stated that information that was 'inaccurate, inadequate, irrelevant or excessive' can be requested by the affected party for removal.

Indian courts have adjudicated on the principle with varying degrees of acceptance and application ranging from the Gujarat High Court[28] denying the existence of such a principle in the Indian constitution to the High courts of Delhi[29], Karnataka and Odisha all granting the right to petitioners. However, the manner in which the principles are being implemented in the absence of a data protection law is unique in the Indian jurisdiction. Judges have chosen a mid way path where they cannot order erasure, where the requested information is not deleted but merely 'de-linked' from search engines and therefore not visible upon normal searches. While such a move balances the right to be forgotten as one where data is not purged but merely buried deeper, there are rudimentary workarounds in place such as the 'Wayback machine' that preserve web pages according to dates and as a result can display them before court mandated edits are put in place.

Recommendations: The right to be forgotten and its implementation by the court need to be streamlined in order to differentiate between de-linking/de-indexing of information from search engines and removal of data at a domain level as they have different connotations and would assist the court to provide proportionate remedies in right ot be forgotten cases.

---

[26] Shekar, K & Venkatesh, K. (2022, August 2) *Positive or zero-sum game: When privacy by design meets dark patterns*. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4178549

[27] Thapliyal,N. (2021, Decemeber 16) *Right To Privacy Includes Right To Be Forgotten, Personal Data Protection Bill Contains Provision For It: Centre Tells Delhi High Court, Live Law*. Retrieved from https://www.livelaw.in/news-updates/right-to-privacy-includes-right-to-be-forgotten-provisions-personal-data-protection-bill-centre-tells-delhi-high-court-187779

[28] *Dharamraj Bhanushankar Dave v. State of Gujarat* (Gujarat High Court) Special Civil Application No. 1854 of 2015

[29] *Jorawar Singh Mundy v. Union of India* (High Court of Delhi) W.P.(C) 3918/2021 & CM APPL. 11767/2021

Secondly, considering that data isn't regulated by a single entity, the Data Protection Authority (DPA) (The Adjudicatory Officer at the DPA was tasked with approving whether a right to be forgotten request stands in the erstwhile data protection bill) will need to harmonise implementation of the right as data can often be regulated by other regulators for instance, RBI regulating financial data. Thus, there is a need to coordinate with other regulatory bodies to ensure the DPA's decision is implemented without transgressing into another regulator's domain.[30]

[30] Shekar,K. (2022, April 22) *Right to be Forgotten in India: What is the Status-quo and Way Forward?*, CXO Outlook. Retrieved from https://www.cxooutlook.com/right-to-be-forgotten-in-india-what-is-the-status-quo-and-way-forward/

The Dialogue™
INFORM ENGAGE IDEATE

The Dialogue™ is a public-policy think- tank with a vision to drive a progressive narrative in India's policy discourse. Founded in 2017, we believe in facilitating well-researched policy debates at various levels to help develop a more informed citizenry, on areas around technology and development issues. The Dialogue™ has been ranked as the world's Top 10 think- tanks to watch out for, by the Think-Tank and Civil Societies Programme (TTCSP), University of Pennsylvania in their 2020 and 2021 rankings.

Recommended citation: Birla, B. & Saxena, G. (2022 September 1) Navigating the Fundamental Right to Privacy in India, The Dialogue™

https://thedialogue.co
https://www.linkedin.com/company/the-dialogue-india/
@_DialogueIndia
https://www.facebook.com/TheDialogueIndia
@thedialogue_offcial