EDITORIAL NOTE

SCRUTINISING THE CRIMINAL PROCEDURE (IDENTIFICATION) ACT, 2022, AND ITS CONFORMITY WITH PRIVACY PRINCIPLES

Aaryan Mithal & Abhinav Gupta[*]

I. INTRODUCTION

The Parliament has recently enacted the Criminal Procedure (Identification) Act, 2022, ('the Act') which seeks to authorise collection, storage, processing and dissemination of sensitive data such as fingerprints, retinal scans, biological samples, amongst others.[1] The Act replaces the erstwhile Identification of Prisoners Act, 1920.[2] Generally, it has been argued that the Act expands the type of data that can be collected, the category of persons from whom it can be collected, and the authority that can authorise such collection.[3]

A petition has already been filed before the Delhi High Court challenging the Act for violating Article 14, Article 19, right to privacy, amongst other grounds.[4] Further, concerns regarding the violation of privacy law in the Indian context have been covered by scholars.[5] In this note, we shall instead attempt

---

[*] Members: Board of Editors, NUJS Law Review.

1 The Criminal Procedure (Identification) Act, 2022, Preamble, §2(1)(b), §4.

2 *Id*., §10(1).

3 PRS India, THE CRIMINAL PROCEDURE (IDENTIFICATION) BILL, 2022, available at https://prsindia.org/billtrack/the-criminal-procedure-identification-bill-2022 (last visited on July 5, 2022).

4 Anushka Jain, *Petition in Delhi High Court Challenges Criminal Procedure Act, Here's Why*, April 26, 2022, available at https://www.medianama.com/2022/04/223-criminal-procedure-act-delhi-high-court-petition-summary/ (last visited on July 5, 2022).

5 Parth Naithani, *The Criminal Procedure (Identification) Bill, 2022*, *and the Right to Privacy*, Vol. 57(16), E.P.W. (2022); Shaoni Das, *The Criminal Procedure (Identification) Act, 2022 Violates Various Constitutional Mandates*, May 19, 2022, available at https://theleaflet.in/the-criminal-procedure-identification-act-2022-violates-various-constitutional-mandates/#:~:text=The%20 2022%20Act%20allows%20police,any%20arrested%20person%2C%20including%20

to focus on three principles of data protection and privacy postulated under the European Union's General Data Protection Regulation, 2016 ('GDPR').[6] These principles are namely the principle of purpose limitation, accountability, and limitation on the storage duration of the collected data. These principles are applicable to the law enforcement authorities and the authorities are mandated to abide by such principles of data protection under the GDPR.[7] The three said principles, as will be argued, reflect the primary concerns that the Act carries with respect to data protection and privacy. It will be accordingly concluded that the Act fails to abide by the aforesaid principles under GDPR.

The relevance and reliance on GDPR for examining an Indian legislation can be drawn on the basis of the judgement in *K.S. Puttaswamy* v. *Union of India* ('Puttaswamy').[8] In this case, the Supreme Court endorsed the data protection principles under the GDPR as being useful for guidance in interpreting the Indian legal framework.[9] Moreover, it is also important to highlight that the principles of data protection present under the GDPR have been adopted through the Data Protection Bill, 2021 ('the DPB').[10] Herein, it is to be noted that the obligations under the GDPR are not directly binding, but it is in the interest of the government to abide by the same since,as stated above, the Indian courts rely on the GDPR for interpretation and the DPB is also based on the same.

At the outset, it is essential to highlight that the State undoubtedly has an interest of national security with respect to the current Act in solving crimes and maintaining public order. However, as noted by the Indian courts, there is a need to balance this interest of the State with the right to privacy, and any infringement of the said right has to be proportional.[11] Herein, this test of proportionality can be determined from the principles laid down under the GDPR.[12] Thus, this test is essentially enforced by abiding with the principles of data protection underlined in the GDPR.[13]

---

convicts (Last visited on July 5, 2022); Project 39-A, An Analysis of the Criminal Procedure (Identification) Bill, 2022, available at https://www.project39a.com/identification-bill (Last visited on July 25, 2022).

6 Regulation (EU) 2016/679 (April 17, 2016).

7 Council of Europe, Practical Guide on the Use of Personal Data in the Police Sector, February 15, 2018, available at https://rm.coe.int/t-pd-201-01-practical-guide-on-the-use-of-personal-data-in-the-police-/16807927d5 (Last visited on July 5, 2022).

8 (2017) 10 SCC 1 ('Puttaswamy').

9 *Id*., ¶65.

10 The Data Protection Bill, 2021, Chapter II.

11 Kamesh Shekhar & Shefali Mehta, *The State of Surveillance in India: National Security at the Cost of Privacy?*, February 17, 2022, available at https://www.orfonline.org/expert-speak/the-state-of-surveillance-in-india/ (Last visited on July 5, 2022).

12 Puttaswamy, *supra* note 8, ¶65.

13 *Id*.

Lastly, it has to be considered that the data which the Act allows to be collected, stored, and processed such as fingerprints, retinal scan, and other genetic data, are categorised as sensitive data under the GDPR and enjoy a greater level of protection as compared to other forms of personal data.[14]

This note intends to shed light on the implications that the Act has on some of the key principles of data protection. Though the DPB is yet to be enacted as a law and has subsequently been withdrawn due to major opposition, it is crucial to abide by the said principles since it has significant impact on an individual's right to privacy.[15] Part II of the note tests the Act against the purpose limitation principle. It concludes that the Act is broad and fails to provide a specific, legitimate, and explicit purpose. Thereafter, Part III proceeds to analyse the storage limitation principle. The note here highlights that the principle needs to be looked in line with the purpose limitation principle so as to provide a specific limit on the retention of data. However, the limits in the Act are highly excessive and do not provide any delineation with a blanket applicability for all data. Part IV of the note focuses on the accountability principle. The part observes that the obligations of data protection can only be imposed when there exist substantial accountability mechanisms on the authorities who process this data. In light of the Act's provisions and an inadequate data protection framework in India, it would be difficult to ensure any of these principles are abided to. Lastly, Part V offers concluding remarks.

II. PURPOSE LIMITATION TEST

This part will first discuss the law, elements and the ambit of the purpose limitation test, before proceeding to apply the same to the Act concerned.

A. THE LAW SURROUNDING THE PURPOSE LIMITATION TEST

Article 5(1)(b) of the GDPR encapsulates the purpose limitation test and states that personal data should be collected for a specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.[16] Herein, it provides an exception of collecting data in public interest, for scientific or historical research or for collating statistics. The said principle and the three elements of specific, clear, and lawful purpose also find mention under the DPB.[17]

---

14 Regulation (EU) 2016/679 (April 17, 2016), Art. 9(1).
15 Puttaswamy, *supra* note 8.
16 Regulation (EU) 2016/679 (April 17, 2016), Art. 5(1)(b).
17 The Data Protection Bill, 2021, §4.

The principle of purpose limitation can be traced back to certain international instruments, namely the OECD Guidelines on Protection of Privacy[18] and the Council of Europe's Convention on the Processing of Personal Data.[19] Even the European Convention on Human Rights, as early as in 1950s provided a basis for the purpose limitation through Article 8. As per the said provision, any interference with an individual's right to privacy would require justification under strictly defined conditions.[20] These conditions arguably constitute a starting point for the principle of purpose limitation since in the absence of a legal basis a legitimate purpose cannot be determined.[21]

The rationale behind the principle is to contribute towards transparency, legal certainty, and predictability.[22] Hence, as per certain scholars, the purpose limitation principle is an outcome of the right to self-determination, i.e. to control how one's personal data is processed and used.[23] The principle aims to prevent the usage of the data in a manner not expected by the individual concerned, while still permitting processing of the data for useful purposes as long as they are legally compatible.[24] Due to such importance, the Court of Justice of the European Union in *Draft Agreement between Canada and the European Union*,[25] highlighted that the principle of purpose limitation which protects against unlawful access and processing is an element of the essence of the fundamental right to data protection. Hence, the purpose limitation principle can be termed as a cornerstone of the data protection regime.

The three elements of the test as mentioned above are specific, explicit, and legitimate purposes. *First*, the specific purpose requirement relates to a form of self-regulation which mandates the controller to have a specified purpose and consider the purpose of the collection of data.[26] This purpose has to be specified before they initiate the collection of data. Moreover, the specification should

---

18 OECD Guidelines on Protection of Privacy, 1980, Guidelines 7, 9-10.

19 Europe's Convention on the Processing of Personal Data, January 28, 1981, E.T.S. No. 108, Art. 5.

20 European Convention on Human Rights, September 3, 1953, E.T.S. No. 5, Art. 8.

21 Nikolaus Forgo et. al, *The Principle of Purpose Limitation and Big Data* in New Technology, Big Data and the Law, 23 (Springer, 2017).

22 Catherine Jasserand, *Subsequent Use of GDPR Data for a Law Enforcement Purpose: The Forgotten Principle of Purpose Limitation*, Vol. 4(2), Eur. Data Prot. L. Rev.,155 (2018).

23 Maria Tzanou, The Fundamental Right to Data Protection: Normative Value in the Context of Counter-Terrorism Surveillance, 40 (Hart Publishing, 1st ed., 2017); Liana Colonna, *Data Mining and its Paradoxical Relationship to the Purpose of Limitation* in Reloading Data Protection, 300 (Kluwer, 2014).

24 Hannes Westermann, Change of Purpose: The Effects of the Purpose Limitation Principle in the General Data Protection Regulation on Big Data Profiling, 47 (Lund University, 2018).

25 Opinion 1/15 of the Court (Grand Chamber) on the Draft Agreement between Canada and the European Union [2017].

26 Art. 29 Data Protection Working Party, *Opinion 03/2013 on Purpose Limitation*, April 2, 2013, 15, available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203en.pdf (Last visited on July 5, 2022).

be precise enough in order to determine the forms of data processing that fall under the purpose and the ones that are excluded.[27] This requirement also depends on the context in which the processing takes place and the number of individuals who are affected by the collection.[28] The crucial question to consider is whether a reasonable person would be able to understand the kinds of processing that will be done on the data. Lastly, if the collection is performed for multiple purposes, each purpose has to be specified individually.[29]

Second, the requirement of explicit purpose in a manner complements the first requirement of specified purpose. This is because, while specified purpose focuses on the establishment of the purposes of the collection, explicit purpose builds on this and states that these purposes have to be communicated to the affected parties in a clear and lucid manner.[30] This is done in order to develop transparency and predictability.[31] It further reduces the risk of the data subject's expectations being different from that of the controller.[32]

Third, the last requirement of a legitimate purpose essentially postulates the existence of a legal ground such as consent of the subject, for collection of the data.[33] It specifies that the purpose must be in accordance with the concerned law, customs, code of conduct and ethics, any other contractual arrangements.[34] Herein, one would need to consider the general circumstances and facts of the case such as the relationship between the data controller and the subject. The ultimate test is to ensure that before any data is collected, there is a legal ground that allows and envisages the collection of such data.[35]

B. APPLYING THE PRINCIPLE TO THE ACT

§4 of the Act permits the collection of measurements such as fingerprints, foot-prints, palm impressions, photographs, iris and retina scan, physical and biological samples, and behavioural attributes.[36] However, it is argued that the Act does not provide a specific, explicit, and legitimate purpose.

---

27 *Id*., 15.
28 *Id*.
29 *Id*., 16.
30 *Id*., 17.
31 *Id*.
32 Zhasmina Radkova Kostadinova, *Purpose Limitation under the GDPR: Can Article 6(4) be Automated?*, 31 (Tilburg University, 2021).
33 Westermann, *supra* note 23, at 19-20.
34 *Id*., 20.
35 *Id*.
36 The Criminal Procedure (Identification) Act, 2022, §4 read with §2(1)(b).

The closest one comes in ascertaining the purpose of such collection of such sensitive data is provided under the Preamble of the Act. It states that the measurements can be taken for the purpose of 'identification' and 'investigation' in criminal matters.[37] However, the ambit of such purpose gets widened under §4 which provides that the collection of data can be done for 'prevention', 'detection', 'investigation', and 'prosecution'. Thus, the scope of the purpose for collecting data is unclear under the Act. For instance, questions can be raised as to whether for the purposes of investigation, the enforcement agencies can access physical and digital spaces such as mobile devices of an individual that is protected by biometric technology such as fingerprints or retina scans. This arguably also raises concernsregarding the legitimacy of such actions and the absence of legal grounds for committing such breach of privacy.

The vagueness in the purpose of collection should also be construed in light of the fact that under §5 of the Act, the Magistrate possesses the power to issue collection of measurements from 'any' individual including one who is not a suspect in the concerned proceeding.[38] Thus, keeping in mind that data under this Act is collected for the purposes of criminal proceedings, and the Act has the capability to affect any individual, it is essential to specify the precise purpose for which such data can be collected. Therefore, the Act fails to precisely and explicitly enlist specific legitimate purposes for the collection of data. Hence, it provides leeway for significant invasion of the privacy of the individual and the protection of data in lieu of the excessively private and sensitive data that is to be collected under the Act.

Recourse can also not be made to §8, which provides for the rule making power of the executive in the form of delegated legislation,[39] to argue that that such specification may be made in the future. This is because it is a well-settled law that delegated legislations cannot address aspects of substantive policy since it is an essential legislative function.[40] Evidently, in the instant case, the purposes for which the data is collected would constitute an issue of substantive policy that would be required to be addressed under the Act itself, instead of its accompanying rules. Moreover, even the listed matters under §8 for which rules can be made relate to matters of procedure and administrative law.

---

37 *Id*., Preamble.

38 *Id*., §5.

39 *Id*., §8.

40 Rajnarain Singh v. Patna Admn. Committee, AIR 1954 SC 569, ¶¶30-32; Registrar, Coop. Societies v. K. Kunjabmu, (1980) 1 SCC 340, ¶¶4-10; Delhi Laws Act, 1912, In re, 1951 SCC 568, ¶189.

III. THE STORAGE LIMITATION PRINCIPLE

After delving into the purpose limitation principle, a linked principle is that of storage limitation. Even if the data collection in this case is considered legitimate under the purpose limitation principle, the principle ascertains a limit on the duration for which the legitimacy can be claimed. This part will provide an analysis on the necessity of storage limitation principle and how it is interlinked to the purpose limitation principle.

A. STORAGE AND PURPOSE LIMITATION INTERLINKED

Article 5(1)(e)[41] of the GDPR provides the basis of the storage limitation principle which states that data should be kept for no longer than is necessary for the purposes for which the personal data are processed.[42] The determination of the purpose can only provide how long the data should be retained.[43] Any excessive usage and storage can only be ascertained if the purpose for the collection has been clearly defined. This is the reason behind why no specific time limit has been provided and is based on the different limits set by the data processors. This entails that data must be erased when the data processing purpose is achieved and hence purpose limitation and storage limitation are both interlinked. A similar exception as mentioned for purpose limitation has been provided here as well. However, adequate safeguards should be made so as to ensure this exception is not misused and the data subjects still have a right.

Similarly, the Modernised Convention 108[44]– a protocol that reaffirms significant data protection principles in Europe – whilst subsequently providing new rights to individuals and increasing the responsibilities of data controllers and data processors also provides key exceptions to the storage limitation principle.[45] They are namely that the exception ought to be provided by law, should respect fundamental rights and freedoms and benecessary and proportionate for pursuing a legitimate aim.[46]

---

41 Regulation (EU) 2016/679 (April 17, 2016), Art. 5(1)(e).

42 Council of Europe, Handbook on European Data Protection Law, available at https://www.echr.coe.int/documents/handbook_data_protection_eng.pdf (Last visited on July 8, 2022).

43 European Data Protection Board (EU) 4/2019 Guidelines on Data Protection by Design and Default (October 20, 2020) ¶53.

44 Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data (May 18, 2018) CM/Inf(2018)15-final, ('Modernised Convention 108').

45 Margot Lens, GDPR & Convention 108: Adequate Protection in a Big Data Era?, Tilburg University (June 8, 2018).

46 Modernised Convention 108, Art. 11.1; Explanatory Report of Modernised Convention 108, ¶¶91–98.

In *S. and Marper* v. *United Kingdom*,[47] the European Court of Human Rights ('ECtHR') specifically placed emphasis on the proportionality of data retention in relation to the purpose of its collection and time limit specifically within the ambit of police control. The ECtHR held that indefinite retention of data such as fingerprints, cell samples and DNA profiling would fail to meet the proportionality test and would be against the principles enshrined in the ECHR. This was due to the fact that the proceedings against the two applicants had been terminated by both acquittal and discontinuances. Hence, storage limitation has significantly gained importance over the years in different contexts with the increase of data collection. It also acts as a restriction on the validity of the justified purpose to ensure that data controllers and processors are not excessively collecting any data under the guise of a legitimate aim.

B. LACK OF STORAGE LIMITATION IN THE ACT

§4 of the Act provides the National Crime Records Bureau ('NCRB') the authority to collect, store, preserve, store, share, disseminate, destroy and dispose records that are measured in pursuance of the provisions of the Act.[48] §4(2) specifically provides that the period for which this measurement shall be retained in an electronic digital form would be seventy-five years.[49] The proviso however states that the measurements of those who have not been previously convicted of an offence and are released without trial or discharged or acquitted by the court, after exhausting all legal remedies would be destroyed. This proviso can also be exempted if a court of Magistrate provides any written reasons for the retention.[50] Hence, the scope of deletion before seventy-five years is only available to a fraction of convicts who are not convicted and are arrested for the first time. Additionally, given that the exhaustion of all legal remedies itself may be a time consuming, costly, and an elaborate process,[51] the data could possibly be retained for a significantly long period.

Even in cases of acquittal it is highly likely that other provisions may still lead to the storage for seventy-five years. For instance, a person is arrested of committing an offence and they refuse to give their measurements. Even if they are acquitted of the offence for which they were initially arrested, they can still be charged for preventing a public servant from performing their duty under §186

---

47 ECtHR, S. and Marper v. United Kingdom, 2008 ECHR 1581.

48 The Criminal Procedure (Identification) Act, 2022, §4.

49 *Id*., §4(2).

50 *Id*., Proviso to §4(2).

51 Law Commission of India, Assessment of Statutory Frameworks of Tribunals in India, Report No. 272, ¶1.3, available at https://lawcommissionofindia.nic.in/reports/Report272.pdf (Last visited on July 5, 2022).

of the Indian Penal Code, 1860. Their measurements would hence be stored for seventy-five years due to the breach of this section. This would imply that anyone who is arrested for any offence and refuses to provide their measurements could possibly have their data stored for seventy-five years, even if their liability is absolved for the offence they were being investigated for initially.[52] This wide ambit of application leaves little room for any exemptions from the law to actually be put in place in practice.

For almost all offenders, the records would exist for a period of seventy-five years regardless of the severity, nature of offence and the sentence imposed on the offender. The retention of data for a long-term period is primarily made with the objective of having a profile of offenders in case they are likely to commit another offence. Having a database of measurements for the same can possibly help in easier tracking, detection and surveillance. However, as of 2020, the recidivism rate of India is at 4.8 per cent.[53] These numbers have only been reducing over time. Given this trend, justifying the storage of data for seventy-five years may not be proportionate and in line with the privacy jurisprudence given by the Supreme Court and foreign jurisdictions.

A blanket period of seventy-five years for 'all' offences without any delineation hence seems excessive, giving the Government the authority to have a repository of the "physical, biological samples and their analysis, behavioural attributes". In the case of *Ople* v. *Torres*, a decentralised national computerised ID reference system had been envisaged by the Government without any limitation on the data to be collected without any specific safeguards. The same was struck down as unconstitutional by the Philippines Supreme Court as it was broad, vague and an overbreadth. It was acknowledged that while States do have the authority to deploy surveillance mechanisms that process data, these cannot impinge on the individual's privacy and have to be drawn with certain limits of the Constitution. Similarly in this situation, while we do not *per se* challenge the objective of the State, we argue that the prescription of excessive data storage periods without any limitation can similarly be broad, vague and an overbreadth by the State.

DNA samples further can be an indicator of an individual's sensitive information such as one's susceptibility to disease, character traits, parentage, kinship which would also involve the data of the relatives who were not a part of the criminal activity that is being investigated.[54] The Act also allows the storage

---

[52] *See* Illustration 2, PRS India, The Criminal Procedure (Identification) Bill, 2022, available at https://prsindia.org/billtrack/the-criminal-procedure-identification-bill-2022 (last visited on July 5, 2022).

[53] Ministry of Home Affairs, National Crime Records Bureau, Recidivism, Ch. 19-C (2020).

[54] Shankar Narayan, *Criminal Identification Bill Follows Similar Unsuccessful, Discriminatory Laws Elsewhere*, THE WIRE, April 12, 2022, available at https://thewire.in/rights/

of data of people who are only incidentally related to the crime which includes witnesses.[55] Hence, reconsideration of the seventy-five years of storage period should be done by the legislators so as to satisfy both the principle of proportionality and the narrow principle of storage limitation. This reconsideration could include prescribing different periods for offences based on their nature. Further, even if excessive time periods are put in place, adequate safeguards and mechanisms to ensure the protection and safety of this data would be required to justify the exception.

IV. THE ACCOUNTABILITY PRINCIPLE

While the previous principles deal with specific obligations on how the data is to be processed, they can only be fully abided by when a mechanism exists which holds accountable the parties that process data. In the absence of such a mechanism, the obligations will have no teeth and would merely be advisory in nature. Hence, the objective of this part would be to apprise the reader with the accountability principle which serves to hold these obligations binding.

A. ESSENTIAL FOR GIVING EFFECT TO ANY OBLIGATIONS

Article 5(2) of the GDPR states that the data controller is to be responsible for demonstrating compliance with the obligations of data protection and the various principles of the same.[56] Furthermore, Article 24 would also requires controllers to implement 'appropriate technical and organisational measures' to demonstrate that the data is being collected in accordance with the principles enshrined in the GDPR.[57] Accountability was adopted as a data protection principle in the OECD guidelines all the way back in 1980 and has continually developed over time.[58]

---

criminal-identification-bill-follows-unsuccessful-discriminatory-similar-laws-elsewhere (Last visited on July 8, 2022).

55 The Criminal Procedure (Identification) Act, 2022, §5; Sanskruti Yagnik & Anubhav Kumar, *A Critique of the Criminal Procedure (Identification) Bill, 2022*, OHRH, April 19, 2022, available at https://ohrh.law.ox.ac.uk/a-critique-of-the-criminal-procedure-identification-bill-2022/ (Last visited on July 8, 2022).

56 Regulation (EU) 2016/679 (April 17, 2016), Art. 5(2).

57 Regulation (EU) 2016/679 (April 17, 2016), Art. 24.

58 Organisation for Economic Cooperation and Development (OECD), *Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, September 23, 1980, available at https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (Last visited on July 8, 2022).

Accountability in general includes two key elements, i.e. the conferring of responsibility and authority, and the answering for the use of that authority.[59] It is an instrument through which once can strike and maintain a balance between the governors and the governed. Given the extensive and sensitive nature of information collected by data processors in this age, the need for accountability only grows further. Even if accountability would not be considered a separate data protection principle until the enactment of the GDPR, the existence of substantive provisions and obligations on the data controller and process are only in furtherance of enabling accountability.[60] Similarly in India, while Governments are allowed to put restrictions on the right to privacy on grounds such as national security and public order, they are to be held accountable for their actions when these are restricted.[61]

Accountability was also considered as a significant factor in the analysis of the Supreme Court in the Puttaswamy decision.[62] It was stated that the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016,provided major functions to the Unique Identification Authority of India ('UIDAI') to carry out functions of data collection.[63] However, it did not place any institutional accountability on the UIDAI to protect the database of citizens' personal information. Emphasis was placed on how "an independent and autonomous authority is needed to monitor the compliance of the provisions of any statute, which infringes the privacy of an individual".[64] Any excesses committed which violate the privacy of the individual would only be achievable when there is an existing regulatory framework to hold the data controller accountable. The accountability principle, therefore, provides individuals a forum to ensure that any obligations and principle that the data controller has to abide to are demonstrated by them explicitly, while also having redressal mechanisms in place in case of any excesses.

B. WHETHER ACCOUNTABILITY IS POSSIBLE WITHIN THE ACT

We believe that to build a framework for accountability these are certain key points that need to be assessed so that the process of collection falls within the principles elaborated upon.

---

[59] T. Joseph Alhadef et al., *The Accountability Principle in Data Protection Regulation: Origin, Development and Future Directions* in Managing Privacy through Accountability, 49-82 (Palgrave Macmillan, 2012).

[60] *Id*.

[61] Lalit Chandok, *Privacy and Data Security – a National Need*, TRAI, available at https://trai.gov.in/sites/default/files/Span_Technology_07_11_2017.pdf (Last visited on July 8, 2022).

[62] Puttaswamy, *supra* note 8.

[63] *Id*., Part H, ¶235.

[64] *Id*.

First, no safeguards have been provided in the Act with respect to the data and how it will be collected, stored, and analysed. As provided above, even if deletion is a mechanism that has been envisaged as a safeguard, it is highly excessive and has not been delineated into specific offences. The lack of any substantive provisions for protection hence itself provides that there will be minimal scope of incorporating any form of accountability. While it may be argued that these safeguards could be provided through the rule-making power as provided in §8, we have highlighted above how such legislation itself can address substantive policy aspects such as privacy and retention of data. Further, given that these rules will be enacted without any existing data protection law until the PDB is passed, it is unlikely that these would be in consonance with the principles discussed in this paper. The management of the data has only been provided to the NCRB – an organisation that has been set up by the government and merely performs the function of acting as a repository of information on crime and criminals to assist investigators. There have been previous concerns regarding the extent of information that has been held by the body and whether there is any accountability for the same.[65] Enactment of such provisions only leads to vesting more surveillance power with these governing bodies and agencies, with no specific authority to deal with privacy violation in case of commission of excesses.

Second, the Act provides that the State Government and Union Territory Administration may notify an appropriate agency to collect, preserve and share the measurements in their respective jurisdictions.[66] No guidelines of accountability and collection of data have been provided with respect to these bodies as well. Their manner of functioning ought to be regulated or prescribed so as to ensure that these bodies similar to the NCRB uphold the right to privacy and data protection.

Third, though India has recognised the right to privacy and resultantly informational privacy in Puttaswamy, it does not have an existing data protection regime that is sufficient. The DPB was deliberated upon and was recently withdrawn by the Central Government.[67] Reconciling the two aims – data protection and investigation of offences – would hence be required while implementing the Act. However, currently the Act has allowed for various exemptions from its provisions when the data processing is undertaken in the interest of national

---

[65] Internet Freedom Foundation, *Guess Who We Heard from? NCRB Responds to IFF's Legal Notice, We Promptly Reply*, November 8, 2019, available at https://internetfreedom.in/the-ncrb-responds/ (Last visited on July 8, 2022).

[66] The Criminal Procedure (Identification) Act, 2022, §4(3).

[67] NDTV, *Government Withdraws Data Protection Bill*, August 3, 2022, available at https://www.ndtv.com/business/data-protection-bill-government-withdraws-data-protection-bill-3221001 (Last visited on August 4, 2022).

security, or for prevention, investigation or prosecution of offences.[68] These trends do not seem highly favourable to all those whose measurements would be taken in pursuance of the Act. Given that the Act's sole purpose is to aid in investigation of offences, it could be likely that the NCRB, police officers and any other agencies constituted at the State and Union Territory levels may be exempted from the provisions of the same. Hence, even if any safeguards could potentially be put in place in a future data protection legislation, the same may not wholly be applicable to the bodies who are in control of the management of such data.

CONCLUSION

In this note, we have discussed the compliance of the Act with the core principles of data protection and privacy as present under the GDPR, namely the principle of purpose limitation, storage limitation, and accountability. The said principles find relevance under the Indian legal framework and are integral in the arena of privacy and protection of data. The concerns herein are numerous and range from the ambit for the purpose for which data can be collected to whether the data controller can be held accountable under the Act.

Hence, as per the above analysis, we believe that the legislation has failed to appropriately balance the interest of national security and the interests of citizens with respect to the protection of their data and their fundamental right to privacy. It particularly becomes crucial to achieve a fine balance in the instant case due to the sensitive data that is sought to be collected as per the Act. Due to such fundamental questions that the Act raises, the outcome of challenges that are made to the constitutionality of this Act before the courts would be crucial in the development of the right to privacy and data protection of Indian citizens.

IN THIS ISSUE

As we approach the nearing end of the COVID-19 pandemic, the new Editorial Board grappled with the resumption of the offline functioning of the NUJS Law Review and brought together Volume 15(1). The Board strives to carry forward the legacy of the previous boards and constructively contribute to the legal academia. The issue would not have been possible without the dedicated effort of our associate members who diligently worked on transforming the initial

---

[68] Joint Committee, Seventeenth Lok Sabha, Report on the Personal Data Protection Bill, 2019, Recommendation 56 (December, 2021); PRS India, *Legislative Brief: Personal Data Protection Bill*, available at org/billtrack/prs-products/prs-legislative-brief-3399 (Last visited on July 8, 2022); Arghya Sengupta, *The Data Protection Bill, 2021: It's No Longer Personal*, Vidhi Legal Policy, available at https://vidhilegalpolicy.in/blog/the-data-protection-bill-2021-its-no-longer-personal/ (Last visited on August 4, 2022).

submissions into publishable articles. Though the greatest asset of the NUJS Law Review shall always be the authors who have once more made valuable contributions in this issue.

Keeping up with this sense of responsibility and commitment, the Editorial Board of the NUJS Law Review for the academic year 2022-23 presents to you this issue consisting of the following five highly researched and brilliantly written submissions covering a wide range of contemporary legal issues.

In their article 'The Impact of the Puttaswamy Judgement on Law Relating to Searches', Pratyay Panigrahi and Eishan Mehta analyse the interplay of the right to privacy with the State's power to conduct searches. Their paper explores the tension between privacy and State authority under criminal procedure. To that end, it comprehensively discusses the legal scenario pre and post-Puttaswamy and emphasises its unique position in Indian privacy jurisprudence. It further utilises comparative jurisprudence to shed light on the manner in which search procedures are construed internationally. Subsequently, the authors provide their recommendations on the manner in which the fundamental right to privacy should be harmonised with the power to search, and argue for a rigorous proportionality analysis for the same.

Devanshi Gupta and Shalini Prem in their article 'Zameen Zameen Ki Ladai: The Contemporary Implications of the Property Law Inconsistencies in 'M. Siddiq v. Mahant Suresh Das' analyse the inconsistencies in the approach taken by the Supreme Court in the case of M. Siddiq v. Mahant Suresh Das, colloquially referred to as the Babri-Masjid-Ram Janmabhoomi dispute. The paper begins by exploring the inconsistencies in the Supreme Court judgement by analysing it from the lens of property law and the Places of Worship Act, 1991. Thereafter, the authors use the Babri-Masjid-Ram Janmabhoomi dispute to show how it can have a huge impact on the ongoing disputes relating to religious properties between Muslims and Hindus. Subsequently, the paper analyses how the recent challenge to section 4(2) of the Places of Worship Act can have widescale implications on all current disputes. Lastly, it highlights how the inconsistent and controversial approach taken by the Supreme Court while considering past evidence and the 'next friend' concept can make future decisions look inherently biased in favour of a particular religious community.

Ashika Jain and Astha Rath in their article 'Analysis of the Indirect Discrimination Test in the Light of COVID-19 Restrictions' analyse whether facially neutral measures can be considered discriminatory in context of the plight of the migrant workers once the lockdown due to COVID-19 was declared. The authors first explore constitutional safeguards against facially neutral measures

with disparate impacts, namely under Articles 14 and 15 of the Constitution. They then analyse the different ways of interpreting Article 15 to include or exclude the concept of indirect indiscrimination. In this regard they discuss the Dworkinian Interpretation, the Scalian Interpretation and Tribe's Interpretation to evaluate the different approaches. The authors also analyse the jurisprudence of indirect discrimination in other countries to establish that clauses which are similar to the text of Article 15 can be interpreted to also prohibit facially neutral measures having disparate impact. The article then goes on to try to establish how Article 15 can be interpreted to bring certain facially neutral measures under its ambit. Finally, the article evaluates the validity of the lockdown in context of its effect on the migrant workers.

Tejas Chhura in his article 'The Need to Re-think the Group of Companies Doctrine in International Commercial Arbitration' discusses the group of companies doctrine *vis-a-vis* its ability to bind non-signatories of an arbitration agreement to the jurisdiction of arbitral tribunals. The paper begins by elucidating the origins of the said doctrine and the degrees to which it has been adopted across various jurisdictions. It then discusses the concept of implied consent and argues that the scope of application of the concept with respect to this doctrine is unreasonably wide. The paper also points to the misapplication of this doctrine by adjudicating bodies and the enforcement issues that arise due to the misapplication. Lastly, the author provides a suggestion to redefine the scope of the doctrine as well as extend the tribunal's jurisdiction without impacting the essence and requirement of consent. The paper concludes with an assessment of the practicality of adopting the suggested approach and the effect it would have on the tribunal, signatories, and non-signatories.

Natasha Gooden, in her article 'COVID-19 and the International Response: An Inquiry into the Possibility of a Global Pandemic Treaty' highlights the lacunae present in public international law with respect to a collective response to the COVID-19 pandemic. The sophisticated and complex nature of international law has been recognised along with a number of areas that need improvement and cooperation between States. She also emphasises the inherent flaws of international law, such as fragmentation and a lack of common enforcement or compliance mechanism. The article also explores the mandates and restrictions placed on the various international organisations. The World Health Organization, the United Nations Security Council, the United Nations General Assembly, and domestic courts are discussed in the article, along with their roles and responses to the pandemic. The paper comes to a conclusion that, despite the fragmented nature of international law, the legal system is flexible enough to change in response to the current pandemic. It contends that holding an international discussion and

creating a ‘Pandemic Treaty’ will demonstrate the potential and the likelihood of international law being effective during future pandemics.

We hope the readers enjoy reading these submissions and welcome any feedback that our readers may have for us. We would also like to thank all the contributors to the issue for their excellent contributions, and hope that they will continue their association with the NUJS Law Review!

Truly,

Editorial Board (2022-2023),

Volume 15 Issue 1

The NUJS Law Review