DATA PROTECTION RIGHTS IN THE AGE OF AI: NAVIGATING THE PRIVACY DILEMMA AND CONFLICTS

Dr. Amitesh Anand[1] & Dr. Ashutesh Anand[2]

ABSTRACT

Today, the rapid expansion and continual evolution of Artificial Intelligence are converging with an unprecedented surge in personal privacy litigation. In India the landmark judgment of *Justice Puttaswamy* not only reshaped the constitutional interpretation of the right to privacy but also redefined the foundational relationship between the individual and the state. This study undertakes a comprehensive doctrinal analysis, comparative constitutional review, and an assessment to measure the real status of available regulations which aims to govern AI. The increasing deployment of AI systems across vital social infrastructures highlights the serious consequences that arise when innovation is pursued without adequate consideration for protecting individual privacy rights and maintaining the legitimacy of democratic governance. This paper worked as a tool that suggests a 'constitutional technology assessment' methodology, which evaluates AI systems against fundamental rights standards.

Keywords: AI, Right to privacy, Supreme Court, Constitution, Puttaswamy Judgment

[1] Dr. Amitesh Anand, Associate Professor, College of Law, IIMT University Ganganagar Meerut
[2] Dr. Ashutesh Anand, Assistant Professor, College of Law, IIMT University Ganganagar Meerut

1. PROLOGUE

Today, the rapid expansion and continual evolution of Artificial Intelligence (hereafter AI) are converging with an unprecedented surge in personal privacy litigation. This intersection is generating complex and far-reaching conflicts, reshaping long-standing legal principles and challenging traditional understandings of individual privacy in ways never before witnessed in modern society. The landmark Judgment of *Justice K.S. Puttaswamy (Retd.) v. Union of India*[3] not only reshaped the constitutional interpretation of the right to privacy but also exerted a profound influence on the Indian legal system, redefining the foundational relationship between the individual and the state. This study undertakes a comprehensive doctrinal analysis, comparative constitutional review, and an assessment to measure the real status of available regulations which aims to govern AI. The requirement to solve this tussle cannot be overstated. The increasing deployment of AI systems across vital social infrastructures highlights the serious consequences that arise when innovation is pursued without adequate consideration for protecting individual privacy rights and maintaining the legitimacy of democratic governance.[4]In this background this paper contends that the privacy paradox can only be overcome through Fundamental change of the both privacy governance and innovation policy. It advocates moving beyond rigid, binary frameworks toward more adaptive, context-sensitive regulatory models that account for circumstantial privacy harms, collective algorithmic impacts, and the systemic nature of data-driven decision-making. Only through the implementation of such thoughtfully recalibrated and context-sensitive framework the legal systems can truly fulfil their dual mandate of protecting fundamental rights and promoting the responsible innovation and responsible technological advancement in current scenario.

2. UNDERSTANDING THE CONSTITUTIONAL STAKES IN THE DIGITAL AGE

In this ongoing era, the accelerating evolution of Artificial Intelligence (hereafter AI) is intersecting with a growing wave of personal privacy litigation, producing a conflict seen never before of unprecedented scope and complexity. In which, currently available AI technology is creating a 'constitutional crisis' and day by day crossing the threshold of a challenge to privacy

[3] Writ Petition (Civil) No. 494 of 2012, (2017) 10 SCC 1; AIR 2017 SC 4161.
[4] Calo, R. (2017). Artificial intelligence policy: A primer and roadmap. University of California, Davis Law Revi ew, 51, 399-435.

jurisprudence.[5] The challenge posed here is not only legal, but also 'algorithmic.' Social 'innovation' and 'algorithmic' innovations are in an intricate dance, and a legal equilibrium will need to test 'human dignity' in unprecedented ways.[6] As the Indian Supreme Court judgement in the Justice *K.S. Puttaswamy (Retd.) v. Union of India*[7] case had not only had a fundamental impact on the interpretation of the constitution, but also it had a powerful impact on the legal system as well on the most fundamental primitive relations of an individual and the state. Most unexpectedly, it was a legal response of such proportions to the new digital technologies, which were at once rapidly transforming the individual data, and relational data, and the state. The recent privacy incongruity arises out of inherent incongruity between AI functionality needs and privacy protection principles. New machine learning tools needs huge database in order to show their capabilities like recognition and predictive capabilities[8]. Such systems are data maximization-based, which fundamentally opposite to the core principles of privacy law that, are data minimization. The paradox becomes even more profound when one thinks about how most societal gains are comes from while AI depends upon the wide-ranging database that contain personal data.

3. CONCEPTUAL PRINCIPLES: UNDERSTANDING PRIVACY IN THE CONTEXT OF CONSTITUTIONAL PARAMETERS

The privacy architecture of the Indian Constitution represents a complex and evolving framework, shaped over decades through jurisprudential development. This is also culminating in the landmark *Puttaswamy verdict* in which Justice Chandrachud stated that three-type categorization of privacy i.e. spatial, decisional, and informational privacy offers a holistic approach of understanding in which AI systems threaten each such type. *Spatial privacy* is threatened in a new manner by AI-driven surveillance systems generating detailed movement histories. *Decisional privacy* becomes an issue when AI uses behavioural forecasting to veto decisions and *Informational privacy* becomes almost impracticable to practice when machine learning algorithms gather sensitive information from harmless data points.[9] This paper worked

[5] Pasquale, F. (2015). The black box society: The secret algorithms that control money and information. Harvard University Press.
[6] Cohen, J. E. (2019). Between truth and power: The legal constructions of informational capitalism. Oxford University Press.
[7] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
[8] Abadi, M., Chu, A., Goodfellow, I., McMahan, H. B., Mironov, I., Talwar, K., & Zhang, L. (2016). Deep learning with differential privacy. Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, 308-318.
[9] Barocas, S., & Selbst, A. D. (2016). Big data's disparate impact. California Law Review, 104, 671-732

as a tool that suggests a "constitutional technology assessment" methodology that analysing AI systems against basic rights standards throughout their life cycle. This model builds on the theme of Nussbaum's capabilities approach to prioritize safeguarding conditions for human flourishing over avoidance of any harm. The dignity-focused model spotlighted in the Puttaswamy judgment offers a further theoretical approach, that setting the categorical boundaries on the AI uses that infringe on human dignity despite of the consent.

This paper worked as a tool that suggests a 'constitutional technology assessment' methodology, which evaluates AI systems against fundamental rights standards throughout their entire life cycle. The model draws on Nussbaum's capabilities approach that focuses on what individuals are able to do and to be – their "capabilities" – rather than merely the resources or utilities they possess. emphasizing the creation and safeguarding of conditions such as life, bodily health, bodily integrity, senses, imagination, thought, emotions, practical reason, affiliation, and control over one's environment, among others for human flourishing rather than merely the avoidance of harm.[10] Additionally, the dignity-focused framework highlighted in the *Puttaswamy judgment* provides a complementary theoretical perspective, establishing categorical boundaries on AI applications that violate human dignity, even in cases of individual consent."

4. AI AND PRIVACY: NAVIGATING THE ALGORITHMIC CHALLENGES

AI frameworks, especially those built on deep learning and neural networks, present privacy challenges that surpass traditional data protection scenarios.[11] Machine learning computations will rely on the enormous data sets and the accuracy increasing algorithms is based on the data size. Training large language models requires processing hundreds of billions of parameters over the trillions of datasets, which may contain personal data without individual knowledge or consent.[12] The most notable "black box society" effects occur most notably in the deep learning algorithms where decision-making processes are unclear even to designers. These 'black-box' systems raise significant concerns for privacy, fairness, and democratic oversight. Neural networks that have millions of parameters to build decision pathways that are not meaningfully translatable into human-understandable form. This ambiguity of

[10] Martha C. Nussbaum, *Creating Capabilities: The Human Development Approach* (Cambridge, MA: Harvard University Press, 2011).
[11] Goodfellow, I., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., Courville, A., & Bengio, Y. (2014). Generative adversarial networks. Advances in Neural Information Processing Systems, 27, 2672-2680.
[12] OpenAI. (2023). GPT-4 technical report.

algorithms violates the transparency and accountability principles rooted in privacy law. On all this certain significant principles regarding transparency and relations between fundamental rights and transparency were set in the judgment of *Anuradha Bhasin v. Union of India*[13] where it was decided that states may not invoke security reasons to justify having full secrecy about surveillance measures. Among these are-

- The *Facial Recognition Technologies* produce "permanent line-ups" where all individuals are potential suspects who are subject to the ongoing surveillance.[14] These technologies illustrate privacy concerns that were raised by AI systems based on ongoing, pervasive data collection.

- The *Predictive Policing Techniques* illustrate how AI systems implant and reinforce in the current social inequalities through discriminatory pattern of discovery, disproportionately will impacting on the marginalized groups; and

- *Automated Credit Scoring Processes* illustrate how AI systems analyse the sensitive financial information in order to make impactful determinations that will influence economic opportunities.

- *Technical writing on privacy-protection AI* demonstrates promise and constraint. Differential privacy offers mathematical proof regarding privacy loss at the expense of accuracy trade-off.[15]Google's RAPPOR system and Apple's implementation prove feasibility with the limited deployment.

- *Federated Learning* supports model training in collaboration without raw data centralization but is susceptible to many privacy attacks. The distance between theoretical potential and practical reality demonstrates larger issues of using privacy-preserving AI. etc.

5. LEGISLATIVE LANDSCAPE: THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023

The Digital Personal Data Protection Act, 2023, is one of the India's most ambitious Act so

[13] Anuradha Bhasin v. Union of India, (2020) 3 SCC 637.
[14] Subhranshu Rout v. State of Odisha, W.P. (Crim.) No. 28 of 2020 (Orissa High Court).
[15] Dwork, C. (2008). Differential privacy: A survey of results. International Conference on Theory and Applications of Models of Computation, 1-19.

far to regulate data processing, but its provisions expose certain primary tensions when used in the context of AI systems. The theme of the Act is based on the notice, consent, and purpose limitation concepts; it is a regulatory philosophy that is crafted for the discrete data processing operations as it is opposed to fluid, repetitive machine learning processes. Section 6 of that Act makes consent of the central legal foundation, mandatory and that consent is "free, specific, informed, unconditional and unambiguous."[16] This model is challenged in AI situations in which algorithms learn purposes and meaning not foreseen at the time of data gathering. The need for express consent assumes that the data controllers will specify clear purposes of that consent, but the machine learning through exploratory analysis produces value only to that emerges in the training process itself. The Act's inaction regarding automated decision-making system stands in pointed contrast under Article 22 of GDPR, which establishes clear rights only for those who are subject to the automated processing decisions. This lacuna is troubling in the context of emerging AI deployment in the high-stakes sectors.[17]The lack of legislation mandating human oversight, transparency over algorithmic decision-making, or a right to appeal algorithmic decisions leaves people open to at the verge of discrimination by algorithms with few avenues for remedy.

The Section 17 the exemption provisions, specifically talks about the national security exemptions[18], by which a broad will be constitute that carve-outs and facilitating the unregulated surveillance of AI deployment. The Act's inability to require proportionality or oversight mechanisms for the purpose of national security exemptions leaves openings for AI surveillance to run completely outside privacy protection regimes. The institutional structure and the organizational framework of the Data Protection Board do not seem sufficiently tackled to meet the technical elegance and the rapid development of complex AI system.

6. COMPARATIVE CONSTITUTIONAL PERSPECTIVES: LEARNING FROM GLOBAL APPROACHES

European Union's dual regulatory model, that is the GDPR and the AI Act, is the most extensive effort at the world level to establish legally binding AI regulationfor the purpose of

[16] Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023).
[17] Calo, R. (2017). Artificial intelligence policy: A primer and roadmap. University of California, Davis Law Review, 51, 399-435.
[18] Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023).

combining privacy safeguard with more general safety and core rights issues. Article 22 of the GDPR has produced a vast jurisprudence clarifying potential and limitations of AI regulation via data protection law. The risk assessment-based strategy of the proposed AI Act offers a graduated regime to strike a balance between incentives for innovation and the protection of fundamental rights. The judgement of the European Court of Justice in Schrems II[19] set out the essential principles of international data transfers with far-reaching consequences for international AI systems. The Court's annulment of the Privacy Shield framework and the focus on the "essentially equivalent" protection of European data being processed outside the region poses problems for AI systems that need worldwide data accumulation. The Google Spain judgement[20]propound the principle of "right to be forgotten," which created special challenges for AI systems whose training was based on the using of past data of the people,which they may wanted to be erased that data later. Machine learning models which represent information in distributed representations, and it is technically impossible for them to remove particular training examples surgically without retraining whole models.

7. JUDICIAL RESPONSES: EVOLVING JURISPRUDENCE ON ALGORITHMIC RIGHTS

The Indian judiciary's stance on AI privacy issues is becoming more defined through landmark judgement that establishes foundational principles for algorithmic accountability. Regarding AI surveillance the case of *Subhranshu Rout v. State of Odisha*[21] is one of India's earliest case in which Orissa High Court's directly inquired into facial recognition. The petitioner objected to the state's deployment of facial recognition without legislative mandate or privacy protection, contending that the potential of that technology for mass surveillance will breach the proportionality requirements set out in the case of Puttaswamy. The court highlighted the need for statutory frameworks, judicial supervision, and technical protection to avoid mission slip. The Supreme Court's view in the incident of internet shutdowns and surveillance practices in *Anuradha Bhasin v. Union of India*[22] gives essential guidelines for assessing AI surveillance systems. Proportionality it reviews for restrictions on fundamental rights, as it is emphasized by the court, moreover it creates a framework that necessitates any

[19] Schrems II (Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems), Case C-311/18, ECLI:EU:C:2020:559.
[20] Google Spain SL v. Agencia Española de Protección de Datos, Case C-131/12, ECLI:EU:C:2014:317.
[21] Subhranshu Rout v. State of Odisha, W.P. (Crim.) No. 28 of 2020 (Orissa High Court).
[22] Anuradha Bhasin v. Union of India, (2020) 3 SCC 637.

measure of surveillance, including AI systems, to be necessary, appropriate, and proportionate to be effective in the pursuingof legitimate objectives. International precedents give very useful lessons in this regard. The judgment of the UK Supreme Court in R (Bridges) v. Chief Constable of South Wales Police[23] showed court's difficulties in the assessing quickly changing AI systems, setting essential standards for legal authorization, policy frameworks, and impactof assessments for biometric surveillance systems.

Developing litigation strategies expose both possibilities and limits of current frameworks for obtaining algorithmic accountability. Public interest litigation has proven to be a vital mechanism for contesting AI deployments impacting significant populations. The creation of algorithmic impact assessments as proof demonstrates significant development in how courts assess technological systems under constitutional norms.[24]

8. PRIVACY-PRESERVING INNOVATION: TECHNICAL AND REGULATORY SOLUTIONS

Fulfilling privacy-by-design principles in AI development necessitates root-level rethinking of system design, data flows, and optimization goals. Ann Cavoukian's original privacy-by-design methodology needs to be modified to combat specific issues of machine learning systems in which data processing arises out of training procedures that find patterns in ways in which it cannot be fully predetermined beforehand. Federated learning systems support model training in collaboration without centralizing sensitive information, and Google's experience in mobile keyboard prediction illustrates viable deployment. Nevertheless, evidence shows federated learning's susceptibility to model inversion and membership inference attacks, requiring supplementary privacy-preserving methods. Homomorphism encryption allows computation directly on encrypted data without decryption, though computational burden continues to be unacceptable for most machine learning use cases.[25]The regulatory framework for the encouragement of privacy-preserving AI use must be properly calibrated. New York City's Local Law 144, mandating bias audits of automated employment decision tools, serves as a model for requiring algorithmic accountability without specifying particular technical means. The suggested Privacy-Preserving AI Certification framework

[23] R (Bridges) v. Chief Constable of South Wales Police, [2020] EWCA Civ 1058.
[24] Article 29 Data Protection Working Party. (2018). Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679 (WP251rev.01).
[25] Gentry, C. (2009). Fully homomorphic encryption using ideal lattices. Proceedings of the 41st Annual ACM Symposium on Theory of Computing, 169-178.

would set technical standards based on ISO/IEC 23053 standards for machine learning platforms and ISO/IEC 23894 for AI risk management. Economic incentives demand consideration of market forces, competitive pressures, and regulatory expenses affecting organizational choice.[26]

9. FUTURE TRAJECTORIES: EMERGING TECHNOLOGIES AND EVOLVING RIGHTS

The modern AI tool like GPT-4 constitute a pattern that inherently compromises with the current privacy norms with their capability to memorize and even recreate the training data. The models, having been trained on large corpora necessarily containing personal data, can reproduce certain training instances word for word, forcing inherent questions about compliance with privacy when trained on web-sized datasets. Experiments have shown that large language models can be induced to disclose personally identifiable information that was present in their training data. Quantum computing implications go far beyond and became threats to encryption to include basic challenges to privacy-preserving technologies assumptions. The exponential speed at which quantum computers can solve some mathematical problems poses the threat of shattering public-key cryptography systems which was used to secure data in transit and at rest. Neurological interfaces pose unprecedented challenges by potentially facilitating direct access to neural signals encoding thoughts, feelings, and intentions, necessitating extension of privacy frameworks to include cognitive liberty and mental privacy.[27] Chile became the first nation to legally safeguard brain activity and mental information in 2021.

Synthetic data creation using methods such as GANs (Generative Adversarial Networks) which provides promise in solutions through the generation of artificial data sets maintaining statistical characteristics without breaching real-person information. Nevertheless, keeping synthetic data from incorporating unintentionally information on actual individuals is still a challenge. The interplay between AI and IoT devices, 5G networks, and edge computing brings

[26] Acquisti, A., &Grossklags, J. (2005). Privacy and rationality in individual decision making. IEEE Security & Privacy, 3(1), 26-33.

[27] Yuste, R., Goering, S., Arcas, B. A., Bi, G., Carmena, J. M., Carter, A., Fins, J. J., Friesen, P., Gallant, J., Huggins, J. E., Illes, J., Kellmeyer, P., Klein, E., Marblestone, A., Mitchell, C., Parens, E., Pham, M., Rubel, A., Sadato, N.,Wolpaw, J. (2017). Four ethical priorities for neurotechnologies and AI. Nature, 551(7679), 159-163.

distributed intelligence environments in which privacy borders become tougher to demarcate and mandate.

10. EPILOGUE

At the outset it is concluded that the privacy paradox, though not only pose difficulties but also resulted into certain challenges. It is not only an insurmountable barrier but also is an encouragement for radical re-conceptualization for how democratic societies regulate the technological advancement in the conformity with the constitutional principles. The conflict arises not from essential incompatibility but from the use of regulatory principles that is developed for sequential data processing to systems working by continuous learning and emergent behaviour.[28] The “Constitutional AI Principles" framework act in a way that it will harmonizes considerations of fundamental rights across all phases of AI creation and use, based on Puttaswamy's dignity-based approach and Nussbaum's capabilities approach. This policy transition from reactive regulation to forward-looking governance requires institutional frameworks with the ability to foresee and block algorithmic harms prior to their manifestation at scale. Good AI governance depends on cooperative action from technologists, legal professionals, policymakers, civil society, and impacted communities. It is not a question of resisting AI innovation but ensuring that it object is to serves constitutional values. Protection of privacy should be seen not as constraint but as essential design principle that encourages public confidence and enables sustainable technological progress.

[28] Kaminski, M. E. (2019). Binary governance: Lessons from the GDPR's approach to algorithmic accountability. Southern California Law Review, 92, 1529-1616.

REFERENCES:

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

2) Pasquale, F. (2015). The black box society: The secret algorithms that control money and information. Harvard University Press.

3) Cohen, J. E. (2019). Between truth and power: The legal constructions of informational capitalism. Oxford University Press.

4) Abadi, M., Chu, A., Goodfellow, I., McMahan, H. B., Mironov, I., Talwar, K., & Zhang, L. (2016). Deep learning with differential privacy. Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, 308-318.

5) Russell, S. (2019). Human compatible: Artificial intelligence and the problem of control. Viking.

6) Calo, R. (2017). Artificial intelligence policy: A primer and roadmap. University of California, Davis Law Review, 51, 399-435.

7) Nussbaum, M. C. (2011). Creating capabilities: The human development approach. Harvard University Press.

8) OpenAI. (2023). GPT-4 technical report.

9) Edwards, L., & Veale, M. (2017). Slave to the algorithm? Why a 'right to an explanation' is probably not the remedy you are looking for. Duke Law & Technology Review, 16, 18-84.

10) Anuradha Bhasin v. Union of India, (2020) 3 SCC 637.

11) Subhranshu Rout v. State of Odisha, W.P. (Crim.) No. 28 of 2020 (Orissa High Court).

12) Shokri, R., Stronati, M., Song, C., & Shmatikov, V. (2017). Membership inference attacks against machine learning models. IEEE Symposium on Security and Privacy, 3-18.

13) Microsoft Research. (2019). Microsoft SEAL: Fast and easy-to-use homomorphic encryption library.

14) Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023).

15) Justice B.N. Srikrishna Committee. (2018). Report of the Committee of Experts on a Data Protection Framework for India.

16) Kaminski, M. E. (2019). Binary governance: Lessons from the GDPR's approach to algorithmic accountability. Southern California Law Review, 92, 1529-1616.

17) OECD. (2019). OECD principles on artificial intelligence (OECD/LEGAL/0449).

18) [40] UNESCO. (2021). Recommendation on the ethics of artificial intelligence (SHS/BIO/PI/2021/1).

19) R (Bridges) v. Chief Constable of South Wales Police, [2020] EWCA Civ 1058.

20) Article 29 Data Protection Working Party. (2018). Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679 (WP251rev.01).

21) ISO/IEC 23053:2022. Framework for artificial intelligence systems using machine learning.

22) Ribeiro, M. T., Singh, S., &Guestrin, C. (2016). "Why should I trust you?" Explaining the predictions of any classifier. Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, 1135-1144.

23) Bundeskartellamt v. Facebook, Case KVR 69/19 (German Federal Court of Justice, 2020).

24) [53] Monetary Authority of Singapore. (2023). FinTech regulatory sandbox.

25) Internet of Things Security Foundation. (2023). Best practice guidelines.

26) European Commission High-Level Expert Group on AI. (2019). Ethics guidelines for trustworthy AI.