INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

 ISSN: 2582-6433

DISCLAIMER

 ISSN: 2582-6433

EDITORIALTEAM

EDITORS

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur.Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board

Dr. Namita Jain

Head & Associate Professor

School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC -NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India.India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time &Utkrisht Bharat Foundation, New Delhi.(2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

 ISSN: 2582-6433

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr.Sagunthala R & D Institute of Science and Technology, Avadi.Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship.He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi.Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi.He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

 ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN

2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

 ISSN: 2582-6433

DATAFIED SELVES: CONSTITUTIONAL PERSONHOOD IN THE AGE OF PREDICTIVE SURVEILLANCE

AUTHORED BY - EARIKA CHIB
Ph.D. Research Scholar (law)
Department of Law, University of Jammu

Abstract:

The advent of the digital era has fundamentally changed how people are viewed, defined, and regulated in both social and legal contexts. The trend of datafication has also increased quantification and analysis of human behavior and identity through digital technologies, being the heart of this change. But there are now major conflicts between constitutional rights and state or corporate authority due to predictive surveillance, which uses big data, artificial intelligence (AI), and algorithms to predict and control possible conduct. Predictive surveillance effects on constitutional personhood, which is a fundamental idea in democracies that recognizes people as rights-bearing beings deserving of autonomy, privacy, and dignity and are examined critically. The research will inquire into the connections between constitutional persons and digital-age predictive surveillance using a doctrinal and comparative legal approach. In order to comprehend how legislators and courts see individual rights in connection to evolving technology, it also aims at examining the main legal sources, including legislation, constitutional provisions, and significant court rulings. Deep insights into various important decisions like Carpenter v. United States and Justice K.S. Puttaswamy v. Union of India will also help in analyzing how legal reasoning changes to accommodate algorithmic profiling and data-driven monitoring. To find legal safeguards and loopholes pertaining to digital identification and surveillance, evaluation of the statutory provisions of globally leading nations will be a significant contributor to the research. Furthermore, the study will evaluate normative gaps and provide practical based solutions for legislative change. Incorporating the word- 'datafied self" which acknowledges that people now exist through digital footprints and algorithmically created identities, the research seeks to rethink constitutional personhood in the digital era. It aims at pinpoint weaknesses in the present legal and constitutional frameworks that do not address the dangers posed by predictive surveillance technologies like algorithmic decision-making and face recognition. The study will also show how these technologies violate fundamental rights. Along with assessing legislative initiatives and court rulings, it will also

 ISSN: 2582-6433

highlight oversight mechanism shortcomings and the judiciary's reaction to technology intrusions on individual liberties. The research will guide legal revisions and offer insights into best practices across globally leading countries. The study will make suggestions for laws and policies in order to protect constitutional personhood in the era of surveillance capitalism.

Keywords: Data, Digital rights, Personhood, Privacy, Surveillance.

Introduction to the concept of datafied self and Surveillance Capitalism

The way people are seen, classified, and governed has undergone significant changes as a result of the digital revolution. The concept of personhood itself is changing dramatically in the modern world, as digital technology increasingly mediates our movements, preferences, conversations, and even thoughts. The idea of the "datafied self" which describes people whose identities and lives are recreated via the collection and algorithmic analysis of data, is a perfect example of this shift.[1] Simultaneously, predictive surveillance with the application of big data, machine learning, and artificial intelligence (AI) to anticipate individual behavior has become a potent, if controversial, instrument in corporate strategy and governance.[2] The act of turning human existence into data for computer analysis is known as "datafication." Every online purchase, GPS ping, swipe, and click adds to a growing body of behavioral data that governments and businesses use to characterize people. These profiles, also known as data doubles, are used to forecast behavior, evaluate risk, and decide who is eligible for services. According to a study by scholar Shoshana Zuboff, this process is known as "surveillance capitalism" in which behavioral prediction is made via commodifying human experience. Wide-ranging ramifications result from the reduction of people to data points, the abstraction and sale of their identities in the opaque markets of predictive analytics. A fragmented, rebuilt representation of a person, the datafied self is put together using machine learning and algorithms.[3] Predictive monitoring thus goes against the conventional understanding of constitutional personhood, which acknowledges people as independent, right-bearing entities deserving of liberty, privacy, and dignity. In countries like the US, the EU, and India, it is necessary to critically analyze the effects of algorithmic monitoring on civil freedoms. This

[1] Sille Obelitz Søe and Jens-Erik Mai, 'Data Identity: Privacy and the Construction of Self' 20 *Synthese* 492 (2022).
[2] Kai Tai Chan, "Emergence of the 'Digitalized Self' in the Age of Digitalization" 6 *Computers in Human Behavior Reports* 100191 (2022).
[3] Yevhen Laniuk, 'Freedom in the Age of Surveillance Capitalism: Lessons from Shoshana Zuboff" 11 *ResearchGate* 67-81 (2021).

 ISSN: 2582-6433

study explores how judicial thinking is changing to handle the new risks presented by data-driven governance, drawing on seminal case laws such as Carpenter v. United States[4] and Justice K.S. Puttaswamy v. Union of India.[5] By embracing the emerging realities of the datafied self, the goal is to suggest a reconsideration of constitutional personhood in the digital age. A powerful example of the perils of datafication is the 2018 Cambridge Analytica incident. Without obtaining informed consent, the business collected information from more than 87 million Facebook users, utilizing it to build psychographic profiles and send personalized political messages to specific people.[6] Important political results, including as the Brexit referendum and the 2016 U.S. presidential election, were influenced by this manipulation. These incidents demonstrate the widespread manipulation of datafied selves, which violates the fundamental principles of constitutional personhood of autonomy, informed choice, and democratic participation.[7]

Predictive Surveillance and its Constitutional Challenges

Algorithms are used in predictive surveillance to forecast future behavior. Although these techniques can improve security and efficiency, they can seriously jeopardize civil freedoms. With little accountability or transparency, predictive algorithms are frequently employed in border security, immigration, police, and welfare distribution. The United States Predictive Policing Programs, such as PredPol, estimate crime hotspots based on past crime data.[8] These systems frequently reinforce and magnify preexisting prejudices in law enforcement, despite being presented as impartial and data-driven. Already overpoliced communities of color are singled out for heightened monitoring, which feeds the criminalization cycle. Due process and equal protection are compromised as a result of algorithmic prejudice. The United States Supreme Court ruled in Carpenter that the government had violated the fourth amendment by obtaining cellphone location data without a warrant. "An intimate window into a person's life, revealing not only his particular movements, but through them his familial, political,

[4] *Carpenter* v. *United States*, 585 U.S. 296 (2018).
[5] *Justice K.S. Puttaswamy* v. *Union of India*, (2017) 10 SCC 1.
[6] Issie Lapowsky, "Facebook Exposed 87 Million Users to Cambridge Analytica", *Wired*, Apr. 04, 2018, *available at*: https://www.wired.com/story/facebook-exposed-87-million-users-to-cambridge-analytica/ (last visited on May 1 , 2025).
[7] "The 2016 Brexit Referendum: A Divisive Turning Point for the UK", *AloneReaders.com*, Nov. 29, 2024, *available at*: https://www.alonereaders.com/article/details/2431/the-2016-brexit-referendum-a-divisive-turning-point-for-the-uk (last visited on May 1, 2025).
[8] "Data Analytics in Crime Prediction and Prevention", *IResearchnet.Com*, *available at*: https://criminal-justice.iresearchnet.com/criminal-justice-process/impact-of-technology/data-an alytics-in-crime-prediction-and-prevention/ (last visited on May 2, 2025).

 ISSN: 2582-6433

professional, religious, and sexual associations, as said by Chief Justice Roberts.[9] This historic ruling recognized the consequences of recognizing data trails as extensions of persons and noted that new privacy rules are needed for digital data.

India's Aadhaar and the Judicial Response

More than a billion people in India are given unique identity numbers under the country's Aadhaar program, the biggest biometric ID system in the world. It was once designed to make welfare distribution more efficient, but it has now developed into a key component of India's digital governance framework. The Indian Supreme Court's nine-judge panel unanimously ruled in Justice K.S. Puttaswamy v. Union of India (2017) that the right to privacy is a basic right guaranteed by Article 21 of the Constitution. The ruling recognized that, in the digital era, information privacy is a component of individual freedom and dignity.[10] The Court underlined that 'the right to control dissemination of personal information' is a component of privacy. Considering the Aadhaar Verdict (2018) and the Puttaswamy (II) follow-up case, the Supreme Court affirmed the legitimacy of Aadhaar in its following five-judge bench decision, although also placed limitations on the scheme. It decided that private services like banking and telecom could not be forced to use Aadhaar.[11] However, there are serious gaps in the protection of the datafied self since the Court did not sufficiently address worries about monitoring and data commercialization.

Global Legislative Approaches and Oversight Gaps

Predictive monitoring is becoming more complicated, yet most legal regimes are still lagging behind. Most governments still fail to accept the datafied self as a constitutional subject.[12] The General Data Protection Regulation (GDPR), which has been in effect since 2018, offers the most extensive data rights framework to date in the European Union. It presents concepts like express permission, purpose limitation, and data reduction. Importantly, people have the right to be free from judgments that are made based only on automated processing, including

[9] *Supra* Note 4.
[10] Ritansha Lakshmi, "Case Summary: Justice K. S. Puttaswamy (Retd.) Vs. Union of India, 2017", *Lawlex.Org*, Apr. 10, 2020, *available at*: https://lawlex.org/lex-bulletin/case-summary-k-s-puttaswamy-retd-v-s-union-of-india-2017/18929 (last visited on May 2, 2025).
[11] Aparajita Balaji, "Case Summary-Justice K.S .Puttaswamy (Retd) vs Union of India", *Law Times Journal*, Mar. 21, 2019, *available at*: https://lawtimesjournal.in/justice-k-s-puttaswamy-retd-vs-union-of-india/ (last visited on May 2, 2025).
[12] Shri Venkatesh, Bharath Gangadharan, *et.al.*, "The Legal Gaps in India's Unregulated AI Surveillance", *The Hindu*, Dec. 18, 2024, *available at*: https://www.thehindu.com/opinion/lead/ the-legal-gaps-in-indias-unregulated-ai-surveillance/article68996389.ece (last visited on May 4, 2025).

 ISSN: 2582-6433

profiling, thanks to Article 22. The datafied self is not specifically mentioned in GDPR, but it is implicitly protected by its protections.[13] On the other hand, China's Social Credit System uses AI, data analytics, and surveillance to track and rank its residents according to their actions. People with poor credit ratings could not be able to travel, have their loans denied, or lose their jobs. Without any constitutional protection, the datafied self is used in this context as an instrument for political compliance and behavioral control. The dangers of unchecked predictive government are shown by the Chinese model.[14]

Algorithmic Prejudice and the Fairness Crisis

Algorithmic bias is a significant problem in predictive surveillance. Artificial intelligence algorithms frequently inherit social biases since they are trained on past data.[15] ProPublica reported that the COMPAS algorithm, which is used to determine recidivism risk in criminal sentencing within the U.S. Criminal Justice System, disproportionately flags Black defendants as high-risk in comparison to white defendants. Under the Fifth Amendment due process provisions and the Equal Protection Clause of the Fourteenth Amendment, these disparities give rise to constitutional problems. In addition to aggravating systemic injustices, biased algorithms jeopardize judicial impartiality.[16] There are constitutional gaps and digital surveillance in India. The use of surveillance technology, including social media monitoring, AI-driven crime mapping, and face recognition systems, has increased in India. India is the world leader in internet shutdowns, for instance, which are frequently excused by claims of public order or national security. These shutdowns violate freedom of speech and the right to life under Articles 19 and 21 by interfering with access to information, education, and basic services, disproportionately harming the concerned states. Panoptic and Facial Recognition Project started by the Internet Freedom Foundation, monitors the use of face recognition technology in India. There is a lack of accountability when there is no legal structure governing such instruments. The datafied self is susceptible to unrestricted monitoring in the absence of legal protections.[17]

[13] Chris Jay Hoofnagle, Bart Van Der Sloot, *et.al.*, "The European Union General Data Protection Regulation: What It is and What It Means" 28 *Taylor & Francis Online* 65-98 (2019).
[14] Nir Kshetri, "China's Social Credit System: Data, Algorithms and Implications" 22 *IEEE* 14-18 (2020).
[15] A. Arora, M. Barrett, *et.al.*, "Risk and the Future of AI: Algorithmic Bias, Data Colonialism, and Marginalization" 33 *Information and Organization* 100478 (2023).
[16] "ProPublica Pioneers Data Journalism to Expose Algorithmic Decision Making Bias", *Factual America*, *available at*: https://www.factualamerica.com/journalistic-landmarks/propublica-pion eers-data-journalism-to-expose-algorithmic-decision-making-bias (last visited on May 6, 2025).
[17] *Supra* Note 12.

 ISSN: 2582-6433

Digital Surveillance and Constitutional Gaps in the Indian Context

With its quickly growing digital environment, India offers several important case studies for comprehending the relationship between constitutional rights and predictive monitoring. For governance, security, and service delivery, the Indian government has depended more and more on digital technology throughout the last ten years. India's digital trajectory shows a pattern of growing state control with not much judicial or regulatory supervision, from the Aadhaar biometric system to AI-powered enforcement tools and face recognition technologies. Not having a strong and complete legislative framework to regulate digital monitoring is one of India's most urgent problems. Despite acknowledging the right to privacy as a basic right in Justice K.S. Puttaswamy v. Union of India (2017), the Supreme Court has been slow to enact legally binding protections against monitoring.[18] Though it did not sufficiently address the extent and consequences of data gathering and monitoring by both state and commercial entities, the following Aadhaar ruling (2018) did offer certain constraints. Another feature of Indian surveillance system is its secrecy. Without sufficient judicial supervision or public openness, laws like the Telegraph Act (1885)[19] and the Information Technology Act (2000), especially Section 69, give the administration extensive monitoring powers.[20] Examples of mass surveillance systems whose reach and operation are still mainly uncontrolled include the Central Monitoring System (CMS),[21] the Network Traffic Analysis (NETRA),[22] and the National Intelligence Grid (NATGRID).[23] The use of the Israeli spyware Pegasus to target Indian journalists, activists, and opposition leaders was made public in 2021. Serious constitutional concerns regarding the misuse of monitoring capabilities were brought up by this discovery, which caused significant indignation. Even when petitions were submitted, the court took a long time to act and the official response was not much convincing. The Supreme Court ultimately reaffirmed that the state cannot use national security as an excuse to avoid judicial scrutiny by appointing an expert committee to look into the matter. But the absence of tangible results demonstrated the judiciary's weak authority in the absence of a thorough legal

[18] *Supra* Note 5.
[19] The Indian Telegraph Act, 1885 (Act No. 13 of 1885.)
[20] The Information Technology Act, 2000 (Act No. 21 of 2000), s. 69.
[21] Jayna Kothari, "The Central Monitoring System (CMS) and the International Principles on the Application of Human Rights to Communications Surveillance", *Centre for Law & Policy Research*, Sept. 23, 2013, *available at*: https://clpr.org.in/blog/the-central-monitoring-system-cms-and-the-international-principles-on-the-application-of-human-rights-to-communications-su rveillance/ (last visited on May 6, 2025).
[22] "NETRA: A Vigilant Eye on the Internet", *Research Matters*, Mar. 08, 2017, *available at*: https://researchmatters.in/article/netra-vigilant-eye-internet (last visited on May 6, 2025).
[23] Vishruti, "A Glance at the National Intelligence Grid (NATGRID)", *Metacept*, Sept. 22, 2020, *available at*: https://metacept.com/a-glance-at-the-national-intelligence-grid-natgrid/ (last visited on May 6, 2025).

 ISSN: 2582-6433

framework.[24]

In India, the application of face recognition technology (FRT) in public areas has been growing quickly. FRT is being used by police agencies in places like Delhi, Telangana, and Uttar Pradesh for crowd monitoring, suspect identification, and even predictive policing. Over 100 face recognition initiatives have been reported by the Internet Freedom Foundation Project Panoptic, many of which were carried out without seeking public input or undergoing legal review. Consent, accuracy, and the possibility of false positives are major issues with these systems, especially when it comes to underserved populations.[25] Initiatives for predictive policing, such the Interoperable Criminal Justice System (ICJS) and the Crime and Criminal Tracking Network and Systems (CCTNS), seek to build interconnected databases to support law enforcement. These techniques run the danger of strengthening preexisting societal prejudices and lack accountability measures, yet being framed as essential for effective enforcement and national security.[26] India is the global leader in enforcing internet shutdowns. The Software Freedom Law Center (SFLC) claims that hundreds of shutdowns have occurred in India in recent years. These shutdowns are typically implemented in advance with little notice. Free expression, assembly, and access to basic services rights guaranteed by Articles 19 and 21 of the Constitution are therefore curbed.[27] The Digital Personal Data Protection Act (DPDP Act) of 2023 is the result of India's recent endeavor to implement a data protection system. The Act is viewed as lacking in numerous important areas, even though it establishes a number of rights for data principals and obligations for data fiduciaries. Most importantly, it gives the government broad exclusions, which contradicts its own professed values of openness and accountability. The Act has drawn criticism for putting state interests ahead of individual rights, It is clear that our understanding of rights in the digital age requires a paradigm shift in the constitution.[28] To acknowledge the datafied self, the conventional theory of personhood which emphasizes the physical, tangible individual must change. The judiciary must

[24] Billy Perrigo, "Governments Used Spyware to Surveil Journalists and Activists. Here's Why Revelations About Pegasus are Shaking up the World", *Time*, July 19, 2021, *available at*: https://time.com/6081433/pegasus-spyware-monitored-journalists-activists/ (last visited on May 6, 2025).
[25] Amber Sinha, "The Landscape of Facial Recognition Technologies in India", *TechPolicy.press*, Mar. 14, 2024, *available at*: https://www.techpolicy.press/the-landscap e-of-facial-recognition-technologies-in-india/ (last visited on May 8, 2025).
[26] "Interoperable Criminal Justice System Making Information Sharing in Judicial System Seamless", *Press Information Bureau*, June 23, 2022, *available at*: https://static.pib.gov.in/WriteReadData/specificdocs/documents/2022/jun/doc202262367401.pdf (last visited on May 9,202 5).
[27] "Internet Shutdowns in India 2022", *Sflc.In*, Dec. 23, 2022, *available at*: https://sflc.in/internet-shutdowns-india-2022/ (last visited on May 9, 2025).
[28] The Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023).

 ISSN: 2582-6433

aggressively interpret fundamental rights to include damages from monitoring and digital identification. The executive and legislative branches must endeavor to create strong frameworks that place a high value on personal responsibility and dignity. India is reaching a turning point. It has the capacity to become a digital superpower, but it also has a duty to protect constitutional rights and democratic principles. Individual liberties are seriously threatened by the unbridled development of monitoring technology, legal issues, and inadequate control. A multifaceted strategy involving constitutional, legislative, judicial, and social elements is needed to address these issues. In the era of predictive monitoring, India can only preserve the integrity of constitutional persons to some point. It is because surveillance technology including face recognition software, AI-powered crime mapping, and social media monitoring are becoming more widely used in India.

Toward a Constitutional Recognition of the Datafied Self

The concept of constitutional personality has to change to consider the reality of the digital age. Conventional legal frameworks ignore the digital imprints that increasingly define identity and agency in favor of focusing on the physical self. Legal Recognition of Digital Personhood as the datafied self must be expressly acknowledged as an extension of personal identity in accordance with constitutional law. This involves admitting that fundamental constitutional rights like privacy, equality, autonomy, and dignity are impacted by digital profiling, algorithmic decision-making, and monitoring.[29] South Africa's emphasis on human dignity provides a comparative perspective. Human dignity is central to the South African Constitution system of rights. This suggests that a rethinking of digital persons can establish dignity as the normative basis for controlling surveillance technology. It is necessary to provide reform recommendations. Adopting thorough Data Protection Laws in various sectors is required as India's newly enacted Digital Personal Data Protection Act and has to be strengthened with more robust protections against data sharing, profiling, and opaque algorithmic choices. There is need to create Algorithmic Oversight Bodies i.e. both public and commercial organizations should be subject to the authority of independent regulatory bodies to audit, examine, and act on algorithmic systems. It should be mandate regarding explainability and transparency. People ought to be able to comprehend and contest algorithmic judgments that impact their rights. Encouraging Digital Literacy and Public Awareness is a must in today's digitally vigilant world. People can successfully exercise their data rights through legal empowerment and public

[29] Ratnesh Kumar Pandey and Manoj Kumar, "Right to Privacy in the Digital Age: Legal Implications and Challenges in India" 8 *Ijlmh* 3098-3124 (2025).

 ISSN: 2582-6433

education initiatives. Encouraging International collaboration is also essentially required. Similar to environmental or human rights treaties, international collaboration is very much necessary to create baseline criteria for digital rights in different sectors.

Initiatives in India and Around the World on Predictive Surveillance and the Datafied Self: Ways to Reform

In response to these concerns, both national and international sectors have started to introduce legislative, judicial, and policy frameworks aimed at protecting individual privacy, dignity, and autonomy in the digital age. However, these initiatives remain fragmented and frequently inadequate in the face of rapid technological advancement. The proliferation of algorithm-driven governance and the exponential growth of digital technologies have changed not only how societies function but also how individuals are defined and controlled. Predictive surveillance, driven by big data and artificial intelligence (AI), has introduced a new paradigm of social regulation that reconfigures constitutional personhood, frequently to the detriment of fundamental rights. Crucially, GDPR's effects have extended beyond national borders, leading businesses, and governments everywhere to adopt its guidelines. In order to guarantee that digital innovation stays in line with democratic and constitutional ideals, it is imperative to examine international and Indian initiatives addressing predictive monitoring. Significant changes have been made at the state and court levels in countries like the United States, despite the lack of a comprehensive federal data protection legislation.[30] Consumers have significant rights regarding their personal data under the California Consumer Privacy Act (CCPA), including the ability to access, remove, and refuse to have their data sold.[31] Carpenter v. United States (2018), a significant decision by the U.S. Supreme Court, led to Digital data as an extension of personality and should be protected by the constitution, according to this ruling. The concerns posed by predictive monitoring have also been addressed by the international community in addition to domestic legislation. Resolutions supporting the right to privacy in the digital era have been approved by the UN Human Rights Council. The UN advocated for moratoriums on AI systems that pose significant dangers to human rights, such as face recognition and predictive policing technology, in its reports from 2022 and 2023.[32] Similarly,

[30] Kamakshi Jasra, "The Global Impact of GDPR: Transformation of the Data Privacy Laws Worldwide", *Lex Talk World*, Aug. 22, 2024, *available at*: https://www.lextalk.world/post/the-global-impact-of-gdpr-transformation-of-the-data-privacy-laws-worldwide (last visited on May 9, 2025).
[31] "What Rights Do Consumers Have Under the CCPA?", *Bloomberg Law*, May 03, 2023, *available at*: https://pro.bloomberglaw.com/insights/privacy/what-rights-do-consumers-have-under-the-ccpa/#consumer-rights (last visited on May 9, 2025).
[32] Daniel J. Powera, Ciara Heavin, *et.al.*, "Balancing Privacy Rights and Surveillance Analytics: A Decision

 ISSN: 2582-6433

the Organization for Economic Co-operation and Development (OECD) released privacy and cross-border data follows rules that emphasize the importance of openness, user control, and responsibility.[33] Canada is among the nations that have taken the initiative. As a component of the larger Digital Charter, Canada's planned Artificial Intelligence and Data Act (AIDA) aims to control powerful AI systems and guarantee algorithmic justice. In an effort to create moral boundaries around AI and data use, it highlights the necessity of openness and risk-based evaluations. But not every country has adopted a democratic route. For example, China's Social Credit System, which assigns residents a score depending on their conduct and directly affects their ability to obtain employment, loans, and travel, has institutionalized predictive monitoring. Despite being technically sophisticated, this paradigm stands in sharp contrast to liberal democratic ideals and serves as an example of how datafication may result in coercive control when rights-based supervision is lacking. A mixed image is presented by the United States. Comprehensive federal data protection regulations are still absent, despite court rulings such as Carpenter v. United States acknowledging the invasive nature of digital spying. States like California have implemented their own data privacy frameworks in the absence of federal regulation. One such framework is the California Consumer Privacy Act (CCPA),[34] which gives citizens certain rights regarding their personal data. However, the structural and systemic problems that surveillance capitalism presents are frequently not adequately addressed by these legislations. It is widely acknowledged that current legal frameworks, which have their roots in the pre-digital and industrial eras, are unable to address the issues of the datafied age. Until the law changes to acknowledge the digital extensions of the individual, the constitutional promises of liberty, equality, and dignity cannot be realized. A person's physical presence is no longer the only thing that defines them. Now, computational representations, digital interactions, and metadata also play a role. Since data is an extension of identity and should be given the greatest level of constitutional protection, we must start treating it as more than just a commodity. This necessitates a paradigm change. Firstly, in order to officially acknowledge digital personality, constitutional concepts need to change. Courts must recognize that algorithmic judgments can impact fundamental rights like equality, due process, and liberty just like human decisions do. Also, lawmakers need to pass thorough and progressive data

Process Guide" 4 *Journal of Business Analytics* 155-170 (2021).

[33] "OECD Issues Revised Privacy Guidelines: Focus on Need for Interoperability", *Hogan Lovells*, Sept. 11, 2013, *available at*: https://www.hoganlovells.com/en/publications/oecd-issues-re vised-privacy-guidelines-focus-on-need-for-interoperability (last visited on May 9, 2025).

[34] "Canada's Artificial Intelligence and Data Act (AIDA) 2024: A Comprehensive Guide", *Cox & Palmer*, Apr. 11, 2024, *available at*: https://coxandpalmerlaw.com/publication/aida-2024/ (las t visited on May 9, 2025).

 ISSN: 2582-6433

protection legislation that gives people real control over their data in addition to preventing abuse. The autonomous regulatory agencies must exist with the authority to examine algorithms, look into violations, and apply sanctions. These institutions need to be politically autonomous, technologically capable, and answerable to democratic ideals. Transparency also needs to be made a legal requirement. Black-box systems that determine everything from criminal risk to creditworthiness need to be transparent and comprehensible.[35] The GDPR's concept of a right to explanation is essential for maintaining procedural justice and accountability. People ought to have the ability to contest algorithmic judgments, request human supervision, and seek compensation for damages incurred. Digital literacy and public involvement are equally important concerning these. Legal rights remain abstract in the absence of a general knowledge of the nature of monitoring and its consequences. The ability to critically and assertively participate in digital governance must be granted to citizens. The media, academic institutions, and civil society groups are essential in promoting this digital consciousness. Lastly, every transformation needs to be firmly rooted in normative principles. Placing human dignity at the core of constitutional interpretation may provide a robust and adaptable benchmark by which new technologies are evaluated, as demonstrated by the South African constitutional experience. More than just being free from monitoring, dignity necessitates having the right to create one's online persona, exercise self-determination, and engage in public life without worrying about being manipulated or profiled.

Conclusion

In summary, we must examine and rethink the concept of the constitutional person in the era of predictive monitoring. A proactive, rights-based perspective that upholds the complete humanity of the datafied self must replace reactive legal remedies. This is a moral need as well as a legal one. Efficiency, convenience, or security must never come at the expense of the freedom to live, think for oneself, and participate actively in public life. Constitutional democracies must adapt to the digital era by making sure that change advances justice rather than dominance, not by opposing it. Reclaiming constitutional personhood for the digital age protects both the democratic thread that unites society and individual liberties. The future of freedom will be fought in legislatures, codebases, and courtrooms rather than on battlefields.

[35] Muhammad Ibnu Sinai, "Deciphering the Black Box: Advancing Creditworthiness and Risk Management Through Explainable AI", *Medium*, Nov. 27, 2023, *available at*: https://medium.com/@sinamuhammad8/deciphering-the-black-box-advancing-creditworthiness-and-risk-management-through-explainable-ai-ae6ef9292333 (last visited on May 9, 2025).

 ISSN: 2582-6433

And it starts with the understanding that every data point represents a human being who is entitled to autonomy, dignity, and constitutional protection.

References

1. A. Arora, M. Barrett, *et.al.*, "Risk and the Future of AI: Algorithmic Bias, Data Colonialism, and Marginalization" 33 *Information and Organization* 100478 (2023).
2. Amber Sinha, "The Landscape of Facial Recognition Technologies in India", *TechPolicy.press*, Mar. 14, 2024, *available at*: https://www.techpolicy.press/the-landscape-of-facial-recognition-technologies-in-india/ (last visited on May 8, 2025).
3. Aparajita Balaji, "Case Summary-Justice K.S .Puttaswamy (Retd) vs Union of India", *Law Times Journal*, Mar. 21, 2019, *available at*: https://lawtimesjournal.in/justice-k-s-puttaswamy-retd-vs-union-of-india/ (last visited on May 2, 2025).
4. Billy Perrigo, "Governments Used Spyware to Surveil Journalists and Activists. Here's Why Revelations About Pegasus are Shaking up the World", *Time*, July 19, 2021, *available at*: https://time.com/6081433/pegasus-spyware-monitored-journalists-activists/ (last visited on May 6, 2025).
5. "Canada's Artificial Intelligence and Data Act (AIDA) 2024: A Comprehensive Guide", *Cox & Palmer*, Apr. 11, 2024, *available at*: https://coxandpalmerlaw.com/publication/aida-2024/ (last visited on May 9, 2025).
6. *Carpenter* v. *United States*, 585 U.S. 296 (2018).
7. Chris Jay Hoofnagle, Bart Van Der Sloot, *et.al.*, "The European Union General Data Protection Regulation: What It is and What It Means" 28 *Taylor & Francis Online* 65-98 (2019).
8. "Data Analytics in Crime Prediction and Prevention", *IResearchnet.Com, available at*: https://criminal-justice.iresearchnet.com/criminal-justice-process/impact-of-technology/data-analytics-in-crime-prediction-and-prevention/ (last visited on May 2, 2025).
9. Daniel J. Powera, Ciara Heavin, *et.al.*, "Balancing Privacy Rights and Surveillance Analytics: A Decision Process Guide" 4 *Journal of Business Analytics* 155-170 (2021).
10. "Interoperable Criminal Justice System Making Information Sharing in Judicial System Seamless", *Press Information Bureau*, June 23, 2022, *available at*:

https://static.pib.gov.in/WriteReadData/specificdocs/documents/2022/jun/doc202262367401.pdf (last visited on May 9, 2025).

11. "Internet Shutdowns in India 2022", *Sflc.In*, Dec. 23, 2022, *available at*: https://sflc.in/internet-shutdowns-india-2022/ (last visited on May 9, 2025).
12. Issie Lapowsky, "Facebook Exposed 87 Million Users to Cambridge Analytica", *Wired*, Apr. 04, 2018, *available at*: https://www.wired.com/story/facebook-exposed-87-million-users-to-cambridge-analytica/ (last visited on May 1, 2025).
13. *Justice K.S. Puttaswamy* v. *Union of India*, (2017) 10 SCC 1.
14. Jayna Kothari, "The Central Monitoring System (CMS) and the International Principles on the Application of Human Rights to Communications Surveillance", *Centre for Law & Policy Research*, Sept. 23, 2013, *available at*: https://clpr.org.in/blog/the-central-monitoring-system-cms-and-the-international-principles-on-the-application-of-human-rights-to-communications-surveillance/ (last visited on May 6, 2025).
15. Kai Tai Chan, "Emergence of the 'Digitalized Self' in the Age of Digitalization" 6 *Computers in Human Behavior Reports* 100191 (2022).
16. Kamakshi Jasra, "The Global Impact of GDPR: Transformation of the Data Privacy Laws Worldwide", *Lex Talk World*, Aug. 22, 2024, *available at*: https://www.lextalk.world/post/the-global-impact-of-gdpr-transformation-of-the-data-privacy-laws-worldwide (last visited on May 9, 2025).
17. Muhammad Ibnu Sinai, ""Deciphering the Black Box: Advancing Creditworthiness and Risk Management Through Explainable AI"", *Medium*, Nov. 27, 2023, *available at*: https://medium.com/@sinamuhammad8/deciphering-the-black-box-advancing-creditworthiness-and-risk-management-through-explainable-ai-ae6ef9292333 (last visited on May 9, 2025).
18. "NETRA: A Vigilant Eye on the Internet", *Research Matters*, Mar. 08, 2017, *available at*: https://researchmatters.in/article/netra-vigilant-eye-internet (last visited on May 6, 2025).
19. Nir Kshetri, "China's Social Credit System: Data, Algorithms and Implications" 22 *Ieee* 14-18 (2020).
20. "OECD Issues Revised Privacy Guidelines: Focus on Need for Interoperability", *Hogan Lovells*, Sept. 11, 2013, *available at*: https://www.hoganlovells.com/en/publications/oecd-issues-revised-privacy-guidelines-focus-on-need-for-interoperability (last visited on May 9, 2025).

 ISSN: 2582-6433

21. "ProPublica Pioneers Data Journalism to Expose Algorithmic Decision Making Bias", *Factual America, available at*: https://www.factualamerica.com/journalistic-landmarks/propublica-pioneers-data-journalism-to-expose-algorith mic-decision-making-bias (last visited on May 6, 2025).
22. Ratnesh Kumar Pandey and Manoj Kumar, "Right to Privacy in the Digital Age: Legal Implications and Challenges in India" 8 *Ijlmh* 3098-3124 (2025).
23. Ritansha Lakshmi, "Case Summary: Justice K. S. Puttaswamy (Retd.) Vs. Union of India, 2017", *Lawlex.Org*, Apr. 10, 2020, *available at*: https://lawlex.org/lex-bulletin/case-summary-k-s-puttaswamy-retd-v-s-union-of-india-2017/18929 (last visited on May 2, 2025).
24. Sille Obelitz Søe and Jens-Erik Mai, 'Data Identity: Privacy and the Construction of Self" 20 *Synthese* 492 (2022).
25. Shri Venkatesh, Bharath Gangadharan, *et.al.*, "The Legal Gaps in India's Unregulated AI Surveillance", *The Hindu*, Dec. 18, 2024, *available at*: https://www.thehindu.com/opinion/lead/the-legal-gaps-in-indias-unregulated-ai-surveillance/article68996389.ece (last visited on May 4, 2025).
26. The Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023.)
27. The Indian Telegraph Act, 1885 (Act No. 13 of 1885.)
28. The Information Technology Act, 2000 (Act No. 21 of 2000), s. 69.
29. "The 2016 Brexit Referendum: A Divisive Turning Point for the UK", *AloneReaders.com*, Nov. 29, 2024, *available at*: https://www.alonereaders.com/article/details/2431/the-2016-brexit-referendum-a-divisive-turning-point-for-the-uk (last visited on May 1, 2025).
30. Vishruti, "A Glance at the National Intelligence Grid (NATGRID)", *Metacept*, Sept. 22, 2020, *available at*: https://metacept.com/a-glance-at-the-national-intelligence-grid-natgrid/ (last visited on May 6, 2025).
31. "What Rights Do Consumers Have Under the CCPA?", *Bloomberg Law*, May 03, 2023, *available at*: https://pro.bloomberglaw.com/insights/privacy/what-rights-do-consumers-have-under-the-ccpa/#consumer-rights (last visited on May 9, 2025).
32. Yevhen Laniuk, 'Freedom in the Age of Surveillance Capitalism: Lessons from Shoshana Zuboff" 11 *ResearchGate* 67-81 (2021).