THE RIGHT TO PRIVACY IN THE AGE OF SURVEILLANCE CAPITALISM: A PUBLIC LAW RESPONSE

Preeti Bhagat, Reva University, Bangalore

ABSTRACT

Surveillance and the right to privacy are frequently viewed as two opposing ideals; one emphasizes individual freedom, while the other emphasizes institutional or governmental security concerns. The study focuses on the goals and evolution of ideas, such as recognizing privacy as a legal right and digital privacy and the technological revolution. The paper also highlights the Indian background in relation to Article 21 of the Constitution. What academics refer to as "surveillance capitalism" has emerged as a result of the quick development of digital technology and data-driven business models, which have turned personal data into a valuable economic asset. Large digital companies are the driving force behind this paradigm, which regularly gathers, tracks, profiles, and monetizes user data often without meaningful consent presenting previously unheard-of obstacles to the constitutional right to privacy. This study explores the conflict between the ubiquitous data extraction methods found in modern digital ecosystems and the basic right to privacy, as guaranteed by Article 21 of the Indian Constitution and upheld in Justice K.S. Puttaswamy v. Union of India. The study assesses the effectiveness of current public law remedies, such as statutory frameworks, judicial interventions, and constitutional protections, using a doctrinal and analytical methodology tackling platform domination, behavioral manipulation, and new types of algorithmic surveillance. The study makes the case that a stronger rights-based framework based on accountability, transparency, and data minimization is required in order to control the unequal power dynamics between individuals and corporate data collectors. In order to ensure that the digital economy develops without jeopardizing individual liberty and democratic principles, the study ultimately suggests a more robust public law response that balances constitutional privacy guarantees with the reality of surveillance capitalism. This study critically looks at how surveillance capitalism, which is supported by the government and corporate actors in India, threatens the right to privacy and, consequently, other essential rights like equality, freedom of expression, and association. It examines how other jurisdictions have struck a balance between economic innovation and privacy protection using a comparative public law lens, and it determines if India's legal system adequately protects

its inhabitants from the exploitative aspects of digital capitalism. “Through a doctrinal and analytical approach, this paper will attempt to prove that in the era of surveillance capitalism, the right to privacy is a moral and democratic necessity rather than just a legal one. While India's continuous digital transformation holds promise for efficiency and progress, it also runs the risk of solidifying a surveillance culture in which people are constantly observed, classified, and influenced. Surveillance capitalism will undermine democratic citizenship itself unless it is offset by a robust public law reaction based on human rights and constitutional morality. Making sure that technology works for people rather than against them is the difficult part. This paper seeks to demonstrate that the growing phenomenon of surveillance capitalism poses a significant threat to the fundamental right to privacy under Indian constitutional law.

Keywords: Right to Privacy, Surveillance Capitalism, Public Law, Data Protection, Constitutional Law, Digital Rights.

STATEMENT OR PROBLEM

India is seeing an unparalleled rise in surveillance capitalism in the digital age, as large private companies routinely gather, examine, and profit from personal information. This data-driven economic model uses behavioral profiling tools, targeted advertising systems, and opaque algorithms to invade extensively into people's private lives, frequently without their meaningful consent. Therefore, rather than the State alone, market-driven technological practices are gradually undermining the constitutional right to privacy recognized in Justice K.S. Puttaswamy v. Union of India. Weak legislative frameworks, insufficient data-protection enforcement, unequal power between users and digital platforms, and low digital literacy all contribute to the problem's exacerbation in India. In exchange for necessary services, citizens unintentionally give up a great deal of personal information, leaving them open to discrimination, manipulation, surveillance, and loss of autonomy. There are serious questions regarding how well public law systems protect privacy from corporate overreach in light of the growing tension between commercial interests and fundamental rights. In order to safeguard India's constitutional right to privacy, it is imperative to investigate how public law might react to, control, and limit surveillance capitalism.

RESEARCH METHODOLOGY

In order to assess the effectiveness of India's public law response and investigate the changing nature of the right to privacy in the context of surveillance capitalism, this study employs a doctrinal and analytical methodology. A doctrinal approach permits a methodical examination of the current

legal materials pertinent to this topic because privacy as a legal concept is firmly anchored in constitutional principles, judicial interpretation, and legislative frameworks. The study only uses secondary sources, such as materials, articles and journals on data protection and constitutional law, scholarly papers, academic commentary, policy reports, and publications from legal think tanks. Secondary literature has also been used to analyze Supreme Court of India jurisprudence and comparative perspectives.

HYPOTHESIS

Surveillance capitalism, driven by unchecked data extraction and monetisation practices of private digital corporations in India, significantly infringes upon the constitutional right to privacy due to inadequate regulatory safeguards and weak public law oversight.

REVIEW OF LITERATURE

1. **Singh & nishith,surveillance capitalism: the price of privacy in the digital age, babasaheb bhimrao ambedkar university, lucknow**

According to the researchers, digital platforms are progressively turning user behavior into data assets, giving rise to new kinds of behavioral prediction and economic power. Such data driven business models, according to Singh and Nishith, depend on opaque permission procedures, leading to a notable disparity between platforms and users. Researchers like Zuboff also emphasize how algorithmic manipulation and microtargeting are used by surveillance capitalism to reorganize autonomy and democratic participation. Additionally, research shows that existing legal frameworks especially in India struggle to keep up with the quick advancement of technology, resulting in regulatory gaps in privacy protection. Studies highlight how increased data surveillance puts marginalized and vulnerable people at disproportionate risk. Comparative research from throughout the world shows that privacy laws differ greatly between countries, making oversight and enforcement more difficult. All things considered, the research emphasizes how urgently strong public-law solutions are needed to protect informational rights in the digital era. The work by Singh and Nishith lacks empirical research into the actual data practices of significant digital platforms, despite its extensive theoretical insights. Additionally, it offers a brief technical study of contemporary data processing techniques including machine learning-driven surveillance and algorithmic profiling. Despite its conceptual strength, the regulatory discussion provides few practical avenues for enforcement in the Indian setting. Additionally, user-centric solutions like

privacy-by-design or digital literacy initiatives receive little attention, and the comparison with worldwide privacy regulations is still brief. These gaps show how much more empirical, technological, and policy-specific research is required.

2. **Yadav & varshney, recalibrating the right to privacy in the digital age: legal challenges and constitutional safeguards in the era of technological intrusion**

According to Yadav and Varshney's analysis, the right to privacy is a dynamic constitutional promise that has to change in tandem with the quick advancement of digital technology. Scholars emphasize privacy as essential to human dignity, autonomy, and political engagement, especially referencing the Supreme Court's historic ruling in Puttaswamy. Research indicates that new technologies like biometric tracking, artificial intelligence, and mass surveillance systems greatly increase invasions of personal and informational privacy. The literature emphasizes the conflict between people' civil freedoms and the state's security goals, particularly as data driven government grows. When compared to international norms like the GDPR, researchers observe that India's present data protection measures are still insufficient. Algorithmic profiling, automated decision-making, and unregulated data processing are identified by a number of authors as emerging constitutional issues that need for greater legislative and judicial clarification. The necessity for strong rights-based digital governance in India is highlighted by comparative research, which shows that privacy safeguards vary greatly between states. The body of research generally agrees that in order to effectively address technological disruption in the digital age, privacy protections must be recalibrated.

INTRODUCTION

Surveillance capitalism has become a powerful force influencing our digital environment in a world where data is the new gold. Businesses are gathering enormous volumes of personal data to support their profit-making tactics, making it harder to distinguish between capitalism and spying. Similar to that nosy neighbor who knows everything about you, surveillance capitalism involves large digital businesses storing your data like it's out of style.

The right to privacy is situated in the nexus of capitalism, technology, and government in the twenty-first century. Once promising democratisation and empowerment of knowledge, the digital revolution has now turned into a system of constant surveillance, which academics like Shoshana Zuboff refer to as "surveillance capitalism." Scholar Shoshana Zuboff invented the phrase

"surveillance capitalism," which has grown to be a powerful force in the digital space, changing how businesses gather and use personal data for financial gain. In this piece, we explore the intricate connection between digital rights and surveillance capitalism. We examine the causes and development of this phenomena, its effects on data security and personal privacy, and the moral issues it brings up.

We also look at the laws and rules that currently regulate data protection in the digital age and suggest ways to protect digital rights in the face of surveillance capitalism's widespread influence.[1] By using personal information as raw material to forecast and influence conduct for financial and political advantage, this new economic system commodifies the human experience. This study shall critically analyse how constitutional democracies like India, where privacy is acknowledged as a fundamental right, the distinction between the voluntary sharing of information and the exploitative extraction of data has grown dangerously hazy within this ecosystem, posing pressing concerns. Despite being quiet on the subject in its original wording, the Indian Constitution has been interpreted by judges to safeguard privacy as a fundamental aspect of Article 21, which guarantees the right to life and personal freedom. The seminal ruling in Justice K.S. Puttaswamy v. Union of India solidified privacy as a fundamental component of autonomy and dignity,offering the legal foundation to fend off intrusions from the government and business. However, in the digital age, this right is under danger like never before. Data collecting and processing have become entangled with market and state operations as a result of India's swift digitisation through programs like Aadhaar and the growing digital economy. While efficiency and inclusivity are the goals of these initiatives, they also make it possible to gather a large amount of personal data about residents, frequently without their knowledge or agreement. Different approaches to this problem are reflected in comparative public law around the world.

ANALYSIS

The General Data Protection Regulation of the European Union offers a thorough framework with a focus on openness, responsibility, and individual consent. However, despite being a big step, the Indian Digital Personal Data Protection Act 2023 gives the government broad discretionary rights to exempt institutions from compliance, which could undermine the fundamental principle of privacy protection. In contrast, the United States is a prime example of a laissez-faire policy, with disjointed sectoral rules that are strongly impacted by business lobbying and financial interests.

[1] David Baker and Lucy Ellis (eds.), Future Directions in Digital Information (lsevier Ltd,2021)

These differences show the intricate link between capitalism, democracy, and privacy: unrestrained surveillance capitalism undermines the fundamental values of freedom and autonomy that public law aims to safeguard, while capitalist enterprises depend on data for innovation. Although the origins of surveillance capitalism may be seen in the early days of the internet, it gained traction with the emergence of tech behemoths like Google and Facebook. By using user data to support their advertising-driven business models, these corporations ushered in a time when surveillance is pervasive in daily digital encounters. [2]

From the standpoint of human rights, privacy is fundamental to individual dignity, freedom of thought, and democratic participation. It is not just a civil liberty. People's freedom to think, speak, and disagree is undermined when they are continuously watched, whether by governments vying for political power or by businesses looking to make money. This has a chilling effect that threatens a country's democratic culture in addition to individual liberty. A perilous fusion of capitalism and authoritarianism is indicated in India by the growing alignment of digital monitoring with political goals, as seen in the form of social media manipulation, targeted advertising during elections, and the purported employment of spyware like Pegasus. It all started innocently enough with targeted advertising, and now it's evolved into a digital labyrinth where our every click is tracked and sold to the highest bidder. Thus, citizens become objects of control rather than subjects of rights when their data is commodified. Digital rights and privacy are significantly impacted by the growth of surveillance capitalism. There are concerns about the deterioration of fundamental rights in the digital sphere because our online activities are continuously tracked and profited from. Surveillance capitalism is not limited to the Big companies. It's the cunning uncle robbing you of your online independence, brother of the digital era. [3] Major organizations, such as banks, government websites, and healthcare providers, have had data breaches due to cyber security lapses. Over 1.16 million cyber security events were reported in India in 2020 alone (CERT-IN, 2021). Sensitive personal information is exposed by these breaches, which can result in financial fraud, identity theft, and reputational damage. The Digital Personal Data Protection Act of 2023 was introduced, but enforcement methods are still inadequate, and fines are frequently insufficient to discourage careless behavior. Securing informational privacy in the digital age requires both individual data protection rights and a robust cybersecurity architecture.[4] Through ecosystems that encompass

[2] Audrey Kobayashi (eds.),International Encyclopedia of Human Geography (Elsevier Ltd, 2020)
[3] Shoshana Zuboff: 'Surveillance capitalism is an assault on human autonomy' available at: https://www.theguardian.com/books/2019/oct/04/shoshana-zuboff-surveillance-capitalism-assault-humanautomomy-digital-privacy (last visited on September 24, 2024).
[4] Solove, Daniel J. and Citron, Danielle Keats, "Privacy Harms", 102 B.U. L. Rev. 793 (2022)

search engines, social media, e-commerce, and smart gadgets, multinational technology corporations like Meta, Google, and Amazon have unprecedented access to consumer data.[5] The surveillance capitalism framework, which entails monitoring user activity to customize advertisements and sway user preferences, is the foundation around which these companies have constructed their business models. These organizations are able to circumvent domestic privacy rules due to a lack of data localization and jurisdictional clarity. Concerns about digital colonialism and consent-based data governance have been raised in India due to the lack of strong legislative control, which has allowed internet companies to profit from user data with little accountability[6].

DATA PROTECTION LAWS AND COMPLIANCE

Data protection regulations aim to prevent your personal information from falling off a cliff and into the wrong hands, much like the guardrails of the digital highway.[7]

On August 11, the DPDP Act 2023 was approved by the Parliament and signed into law by the President. The regulation covers "digital personal data," which includes both offline and digitally gathered personal information. It also covers international organizations that handle people's personal information in India (for instance, if they provide services to Indian consumers). Compliance with the DPDP framework for companies, organizations, or any other body handling personal data in India entails: establishing internal data-handling guidelines that specify what personal information is gathered, why, for how long, and how consent is obtained, gaining informed consent prior to data collection and making sure privacy notices are transparent and unambiguous. Minimizing data acquisition means gathering only what is required putting strong security measures in place, such as encryption, access controls, frequent audits, and safe data storage. Enabling users to access, update, remove, or file complaints is known as facilitating data-principal rights upholding breach-response procedures, which include keeping an eye out for breaches and swiftly alerting DPBI and impacted parties in the event of a security incident or unauthorized disclosure. Appointing a Data Protection Officer, conducting Data Protection Impact Assessments on a regular basis, and evaluating data processes are all necessary for organizations managing high quantities. Verifiable parental or guardian consent is one of the special compliance requirements for sensitive

[5] Eubanks, Virginia, Automating Inequality: How High-Tech Tools Profile and Police punish the poor, St. Martin's Press, New York

[6] Bhatia, Gautam, "India's Executive Response to COVID-19", The Regulatory Review, May 4, 2020, available at: https:/www.theregreview.org/2020/05/04/Bhatia-indias-executive-response-covi-19/

[7] The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power available at: https://www.hbs.edu/faculty/Pages/item.aspx?num=56791 (last visited on September 24, 2024).

data classes (like children's data). Governments are under growing pressure to implement stricter laws to safeguard digital rights and stop the abuses of surveillance capitalism as worries about data privacy increase.

EVOLUTION OF THE RIGHT TO PRIVACY IN INDIA

Prior to being elevated to fundamental status due to technical improvements, the right to privacy was a secondary constitutional matter. The ruling of Justice K.S. Puttaswamy v. Union of India marked a significant turning point in the Indian constitution.[8] The ruling established privacy rights under Article 21. The digital era has brought up a number of sophisticated dangers to privacy rights, including state level monitoring and predictive law enforcement as well as business information collecting through AI systems. The right to privacy is both essential and constantly in jeopardy in our digital age culture. The fundamental value of privacy evolved from its peripheral civil liberty position in old democracies to become a central component of democratic constitutionalism as digital technology advanced widely and gained control. The widespread availability of cellphones, biometric systems, data analytics, surveillance cameras, and artificial intelligence provide new privacy risks to people. An important constitutional milestone was reached in India when the right to privacy was acknowledged as a fundamental right in Justice K.S. Puttaswamy v. Union of India. However, the difficulties presented by corporate data monetization, algorithmic profiling, and state surveillance programs must now be evaluated. [9][10] The right to privacy has been gradually recognized by India's constitution. In Kharak Singh v. Singh v. State of Uttar Pradesh[11], the Supreme Court initially took a narrow stance and rejected privacy as a basic right. In the end, the Court recognized a penumbral right to privacy under Article 21, most notably in Gobind v. State of Madhya Pradesh[12]. A nine-judge panel unanimously found in the landmark decision in Justice K.S. Puttaswamy v. Union of India that the right to privacy is intrinsically tied to the right to life and personal liberty under Article 21 of the Indian Constitution. [13] Indian privacy law underwent a sea change after the Supreme Court's decision in Justice K.S. Puttaswamy v. Union of India[14]. As part of the right to life and personal liberty, the nine-judge panel unanimously decided that the right to

[8] Justice K.S Puttaswamy v. Union of india
[9] Ibid 8
[10] Chandrachud D.Y. (2017) Justice K.S Puttaswamy (Retd), Union of india, supreme court of india, W.P, (Civil) No. 494 of 2012.
[11] Kharak singh v. state of uttar Pradesh (1962) AIR 1963 SC 1295
[12] Govind v. state of Madhya Pradesh, 1955 CrLJ 1275,
[13] Lundberg, Ian, Narayanan, Arvind, Levy, Karen, and Salganik, Matthew. "Privacy, Ethics, and Data Access: A Case study of the Fragile Families Challenge" Socius: Sociological Research for a Dynamic World, vol. 4, 2018, pp. 1-13.
[14] Supra 8

privacy is a basic right under Article 21 of the Constitution[15]. The decision emphasized that privacy encompasses a range of protections, including autonomy in making decisions, informational self-determination, and physical integrity. It created the triple standards of legality, need, and proportionality for any governmental interference with the right to privacy, drawing inspiration from international law such as the Canadian Charter and the European Court of Human Rights[16]. However, the right was primarily aspirational at the time because there was no particular privacy statute. The amount of personal data generated online has skyrocketed since the introduction of Web 2.0 platforms.

Large volumes of user data are gathered by social media companies, frequently via cookies and unclear terms of service[17]. As seen in the Cambridge Analytica controversy, data mining and big data analytics enable businesses and governments to profile people, forecast behavior, and even affect decision-making processes[18]. The risk of user data being commodified is increased by the absence of effective data protection legislation. This behavior challenges democratic discourse and autonomy in addition to undermining informational privacy[19]. The way that personal data is handled and used has changed dramatically as a result of artificial intelligence. Automated employment tools, credit scoring systems, and predictive policing algorithms all function with little transparency and frequently incorporate biases and mistakes[20]. These systems violate the concepts of accountability and fairness by making important judgments based on datasets that may not have been properly anonymized or gathered with consent[21]. In the Indian context, ethical frameworks and legal protections are desperately needed due to worries about AI-driven surveillance in law enforcement and benefit programs like Aadhaar[22].

CONCLUSION

In conclusion, the relationship between digital rights and surveillance capitalism offers a complex

[15] Sarat, A and Silbey, S.S., "The pull of the policy audience",10(2-3) Law and Policy 97-166 (1988)
[16] Bhatia, G. (2018). The Transformative Constitution: A Radical Biography in Nine Acts. HarperCollins India
[17] Tufekci, Zeynep, "Algorithmic Harms Beyond Facebook and Google: Emergent Challenges of Computational Agency", 13 Colo. Tech. L.J. 203 (2015)
[18] Isaak, Jim and Hanna, Mina J., "User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection", 51 Computer 56 (2018)
[19] Zuboff, Shoshana, The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power, Public Affairs, New York (2019)
[20] Eubanks, Virginia, Automating Inequality: How High-Tech Tools Profile and Police punish the poor, St. Martin's Press, New York (2018)
[21] Crawford, Kate and Paglen, Trevor, Excavating AI: The Politics of Images in Machine Learning Training Sets, (2019) available at https://excavating.ai/
[22] Ramanathan, Usha, "Aadhaar and the Right to Privacy", 13 Indian J. Const. L. 1 (2021)

issue that calls for constant debate, investigation, and lobbying. In order to preserve a balance between technical progress and ethical considerations, it is imperative that individuals and policymakers prioritise the preservation of privacy and personal data. In the face of widespread surveillance capitalism, we may work towards a future where digital rights are honoured and preserved by remaining informed, having conversations, and supporting strong data protection laws.[23] Technological solutions are essential to protecting privacy since surveillance capitalism depends on gathering and analyzing enormous volumes of personal data. There are solutions available to assist consumers protect themselves, such as VPNs, ad blockers, and encrypted chat apps, their information from prying eyes. People can limit the scope of surveillance capitalism and protect their digital liberties by utilizing these technologies. In conclusion, maintaining individual privacy and digital rights in the present period is severely hampered by the growth of surveillance capitalism. In order to empower people and safeguard their privacy, stakeholders must prioritize ethical issues, support strong data protection legislation, and use technology solutions. By taking proactive measures to address these problems, we can work toward a more equitable and rights respecting digital ecosystem for all. [24] The way the digital world functions has been altered by surveillance capitalism, which has made personal data a commodity that businesses may benefit from. Serious ethical concerns are brought up by this approach, particularly with regard to personal control and privacy. Although certain data protection legislation exist, but effectively implementing them is still challenging, particularly given the influence large tech corporations have. All stakeholders, including legislators, activists, and regular users, must work to defend digital rights. We may contribute to preventing the exploitation of personal data by advocating for improved legislation and employing privacy-protecting technologies. Going forward, it's critical to be vigilant and advocate for more robust safeguards in the digital age. [25]

[23] 'The goal is to automate us': welcome to the age of surveillance capitalism available at: https://www.theguardian.com/technology/2019/jan/20/shoshana-zuboff-age-of-surveillance-capitalism-googlefacebook (last visited on September 24, 2024).
[24] Singh & Nishith, SURVEILLANCE CAPITALISM: THE PRICE OF PRIVACY IN THE DIGITAL AGE, Babasaheb Bhimrao Ambedkar University, Lucknow
[25] Ibid 6