Synergy: International Journal of Multidisciplinary Studies
Vol. 2. **Issue** 2, 2025. Pp. 52-64
ISSN: 3048-7005

Article

From Data to Discrimination: Gender, Privacy, and the Politics of Digital Surveillance

Mahera Imam[1*] **N. Manimekalai, S. Suba**

1. *Research Scholar, Department of Women's Studies, Khajamalai Campus, Bharathidasan University
Email: maheraimam8@gmail.com
2. Director, Centre for Women's Development Studies, New Delhi
3. Professor, Department of Women's Studies, Khajamalai Campus, Bharathidasan University

Article History

Received: 25-05-2025
Revised: 09-06-2025
Acceptance: 13-06-2025
Published: 15-06-2025

DOI: 10.63960/sijmds-2025-2262

Abstract

A greater amount of surveillance of gendered populations has been brought about as a consequence of the era of datafication, which has the effect of reinforcing the structural forms of inequality that already exist. Taking a critical look at the ways in which surveillance capitalism and algorithmic governance turn privacy into a contentious domain, with a disproportionate impact on women and communities that are excluded, this article examines the ways in which these two factors exacerbate the problem. The purpose of this study is to analyse the ways in which well-established patriarchal and racial biases contribute to the growth of digital vulnerabilities using technology such as facial recognition and predictive policing. In order to accomplish this, it makes use of feminist theories and publications that have been issued by Amnesty International (2022) and the United Nations Women (2023). The digital panopticon has the effect of expanding offline oppression into digital domains so that it can be experienced by a greater number of people. This is in contrast to the data colonialism, which greatly restricts autonomy, particularly in the Global South. Particularly in light of the expansion of cyberstalking, doxxing, and bias guided by artificial intelligence, the absence of gender-sensitive digital regulations continues to be a significant cause for worry. In order to argue that surveillance is a political act of control and to suggest that intersectional digital rights frameworks should be implemented, the goal of this study is to be conducted. It accomplishes this by addressing feminist criticisms that have been made in the past. This organisation seeks to reimagine privacy as a social and feminist concern in the digital age. Its mission is to work for systemic reforms in the fields of law, technology, and policy for the purpose of achieving this goal.

Keywords: Datafication, Surveillance Capitalism, Algorithmic Governance, Data Colonialism, Feminist Digital Rights, Women Empowerment

INTRODUCTION

Contextualising Datafication and Gendered Surveillance

The digital age has witnessed an unprecedented shift in how data is collected, processed, and utilised, a phenomenon referred to as 'datafication' (Van Dijck, 2014). Datafication refers to the transformation of human actions and identities into quantifiable data (Van Dijck, 2014), while gendered surveillance highlights how these processes disproportionately monitor and regulate women and marginalised identities. This process transforms human behaviours, interactions, and identities into quantifiable data points, often without individuals' explicit consent. While datafication is presented as a neutral and inevitable aspect of technological advancement, feminist scholars argue that it is deeply embedded within existing structures of power and control (Dubrofsky & Magnet, 2015). One of the key concerns arising from datafication is gendered surveillance, where digital technologies disproportionately monitor and regulate women and other marginalised groups. The feminist critique of surveillance highlights that digital monitoring is not merely a tool for security but a mechanism of

social discipline and control (Foucault, 1977). The expansion of surveillance technologies ranging from facial recognition to algorithmic policing mirrors and amplifies the patriarchal scrutiny historically imposed on women's bodies and behaviours (Chun, 2006). As Couldry and Mejias (2019) describe, this transformation signals the emergence of "data colonialism," where data extraction perpetuates new forms of exploitation and governance over marginalised communities. Gendered surveillance operates across both public and private spheres, reinforcing patriarchal control by disproportionately targeting women and marginalised groups. It entails the unequal monitoring and regulation of individuals based on gender, perpetuating existing social hierarchies through biased technologies and discriminatory practices. In public spaces, women are subjected to extensive scrutiny through CCTV cameras, biometric identification, and predictive policing, which disproportionately profile them as victims or deviants. In private domains, the increased use of digital tracking in intimate relationships, such as stalker ware and coercive control through technology, demonstrates how digital tools facilitate gender-based violence (Dragiewicz et al., 2018). The pervasiveness of these technologies raises urgent questions about agency, autonomy, and the right to privacy in the digital age.

The Rise of Surveillance Capitalism and Its Impact on Privacy

The commodification of personal data has given rise to what Shoshana Zuboff (2019) defines as "surveillance capitalism"—a system in which corporations extract behavioural data to predict and influence future actions. This economic model transforms users into sources of raw material for data-hungry platforms, where privacy is no longer a fundamental right but a contested domain shaped by corporate and state interests. Surveillance capitalism is particularly insidious in its gendered implications, as it exploits women's digital footprints to reinforce consumer profiling, algorithmic biases, and targeted advertising that often perpetuate sexist and discriminatory norms (Noble, 2018). A stark example of such capitalism is the algorithmic discrimination embedded in AI-driven surveillance systems. Studies have shown that facial recognition technologies exhibit higher error rates when identifying women, especially those of colour, leading to cases of misidentification, wrongful arrests, and exclusion from digital spaces (Buolamwini & Gebru, 2018). The growing dependence on predictive policing algorithms disproportionately targets marginalised communities, thereby perpetuating systemic inequalities in law enforcement practices (Eubanks, 2018). Beyond state surveillance, the corporate surveillance ecosystem dominated by big tech companies such as Meta (Facebook), Google, and Amazon monetises intimate data, from reproductive health tracking to online search behaviours. The post-Roe v. Wade era in the United States has already demonstrated the dangers of digital surveillance for reproductive rights, where data collected from period-tracking apps and search histories has been weaponised against women seeking abortions. This highlights how gendered surveillance extends beyond privacy violations to actively police women's bodies and choices.

Significance of Studying Gendered Dimensions of Digital Surveillance

The intersection of gender and surveillance is a critical site of inquiry, as digital technologies are not neutral but actively reinforce historical and structural inequalities (Gandy, 1993). As surveillance infrastructures expand globally, the burden of constant monitoring, policing, and discipline falls disproportionately on women and marginalised communities. Feminist digital rights advocates argue that digital surveillance is an extension of patriarchal oppression, where the digital realm mirrors the traditional mechanisms of control imposed on gendered bodies (Bivens & Haimson, 2016). This issue is particularly pressing in the Global South, where authoritarian governments increasingly deploy digital surveillance under the guise of national security. Research indicates that women activists, journalists, and human rights defenders face heightened risks of state-led digital harassment, hacking, and surveillance (Amnesty International, 2022). The rise of doxxing, cyberstalking, and AI-driven discrimination further exacerbates gendered vulnerabilities, exposing women to public shaming, blackmail, and violence (Citron & Chesney, 2019). Understanding these gendered dimensions is vital for developing inclusive and equitable digital policies. Existing legal frameworks such as the General Data Protection Regulation (GDPR) in Europe and India's Digital Personal Data Protection Act (2023) fail to adequately address gendered privacy violations, leaving significant gaps in protection against algorithmic bias and data exploitation. Addressing these concerns requires intersectional feminist approaches that challenge surveillance capitalism, advocate for data justice, and push for gender-sensitive digital governance models (Couldry & Mejias, 2019).

METHODOLOGY

This research paper is a conceptual analytical review paper. The arguments have been derived from the works of different literature published in the area, such as gender digital rights, digital surveillance, and data colonialism, and secondary data has been analysed using the UN Women's Gender and Technology Report (2023) alongside recent related reports. The findings underscore the importance of creating more inclusive and equitable digital environments that prioritise gender perspectives.

OBJECTIVE OF THE PAPER

This paper aims to contribute to this discourse by critically analysing the intersection of gender, privacy, and digital surveillance, exploring how contemporary technologies exacerbate discrimination, and arguing for a more inclusive and feminist digital rights framework. The paper is structured as follows: Section 2 outlines the theoretical framework, Section 3 presents empirical illustrations, Section 4 explores the political economy of surveillance, and the final section offers recommendations for feminist digital governance.

THEORETICAL FRAMEWORK

Understanding the intersection of gender, privacy, and digital surveillance requires a robust theoretical foundation that critically examines how surveillance technologies perpetuate systemic inequalities. This section draws on four key theoretical perspectives. Surveillance capitalism, algorithmic governance, the digital panopticon, and data colonialism to illuminate the gendered dimensions of contemporary surveillance practices..

Surveillance Capitalism: Data as a Tool of Control

Shoshana Zuboff (2019) defines "surveillance capitalism" as an economic system where personal data is harvested, commodified, and monetised by corporate entities to predict and manipulate human behaviour. Unlike traditional capitalism, which revolves around production and exchange, surveillance capitalism operates by extracting human experiences as raw material for data-driven profit. In the context of gendered surveillance, capitalism exacerbates existing power hierarchies. Women, particularly those from marginalised communities, face heightened risks as their data is used to reinforce gender stereotypes, target them with exploitative advertising, and monitor their behaviour. Studies indicate that predictive algorithms disproportionately profile women based on traditional gender roles, influencing everything from online job advertisements to loan approvals (Lambrecht & Tucker, 2019). Feminist scholars argue that data-driven surveillance deepens digital inequalities by making women's online behaviours more visible and susceptible to exploitation (Dubrofsky & Magnet, 2015). For instance, the targeted collection of intimate data such as menstrual cycle tracking and pregnancy-related searches has led to policing of women's reproductive rights, particularly in the post-Roe era in the U.S.. This case demonstrates how gendered surveillance is not just a privacy issue but a broader mechanism of social control.

Algorithmic Governance: Gendered Biases in AI and Predictive Policing

Safiya Noble (2018) explores how algorithmic governance, the use of AI, and data-driven decision-making systems reinforce gender and racial biases. Algorithms are often perceived as neutral and objective, yet they are trained on historically biased datasets that disproportionately misidentify and discriminate against women and people of colour (Buolamwini & Gebru, 2018). One of the most alarming aspects of algorithmic governance is its role in predictive policing. Studies indicate that AI-driven policing systems disproportionately target communities with a history of structural marginalisation (Eubanks, 2018). Women, particularly those from Black, Indigenous, and Dalit backgrounds, are more likely to be flagged as "high-risk" in AI-driven surveillance despite systemic underreporting of crimes against them. Automated content moderation systems on social media disproportionately silence women and LGBTQ+ individuals. Research has found that women speaking about gender-based violence or feminist activism are more likely to have their posts flagged as "offensive" or "harmful" compared to men posting hate speech (Gillespie, 2018). This phenomenon reflects what Noble (2018) calls the "algorithmic oppression" embedded in big data structures, where digital tools become gatekeepers of visibility and participation.

The Digital Panopticon: Extension of Patriarchal Monitoring into Digital Spaces

Michel Foucault (1977) introduced the concept of the panopticon to describe a surveillance structure where individuals internalise self-discipline due to the constant threat of being watched. In the digital age, this notion has evolved into the digital panopticon, where ubiquitous monitoring mechanisms track women's online and offline movements, reinforcing patriarchal control. In patriarchal societies, digital surveillance functions as a modern-day form of social discipline, policing women's behaviours, mobility, and speech. Examples include family-imposed digital surveillance, where women's online activities are monitored by partners or relatives through spyware and tracking apps (Dragiewicz et al., 2018). State-imposed digital surveillance, where authoritarian regimes monitor and suppress women activists and journalists through hacking, online harassment, and digital blacklisting (Amnesty International, 2022). This digital policing extends beyond the individual level, shaping societal norms of femininity and respectability. Women engaging in political discourse or activism online often face intense trolling, doxxing, and cyberstalking, forcing them to self-censor or withdraw from digital spaces (Banet-Weiser, 2018). This reinforces offline structures of gendered oppression, as women's presence in public discourse is diminished through digital intimidation.

Data Colonialism: The Exploitative Nature of Data Extraction

Nick Couldry and Ulises Mejias (2019) introduce the concept of 'data colonialism' to describe how data extraction operates as a new form of colonial domination, disproportionately exploiting individuals in the Global South. Just as historical colonialism depended on resource extraction and exploitation, data colonialism thrives on harvesting personal information without consent, particularly from marginalised communities.

For women in the Global South, data colonialism manifests in multiple ways:

- Increased state surveillance, where authoritarian regimes use digital tracking to suppress women's rights movements and activism.
- Exploitative data policies by tech giants, where corporations like Meta (Facebook) and Google extract vast amounts of data from women users in low-income regions under the guise of "free internet access" (Couldry & Mejias, 2019).
- Lack of data protection laws, which leaves women vulnerable to misuse of their personal information, including non-consensual image sharing and AI-driven discrimination (Citron & Chesney, 2019).
- Feminist scholars argue that data colonialism reinforces digital dependency, where women's participation in online spaces comes at the cost of constant surveillance and exploitation. Addressing this requires an intersectional feminist approach to data governance, ensuring meaningful consent, ethical AI development, and data sovereignty for marginalised populations (Gurumurthy & Chami, 2021).

GENDER, PRIVACY, AND DIGITAL SURVEILLANCE

The intersection of gender, privacy, and digital surveillance exposes the structural inequalities embedded in technological governance. Women and marginalised communities are disproportionately subjected to heightened scrutiny, AI-driven discrimination, and cyber-based threats such as cyberstalking and doxxing. Drawing from contemporary reports, such as UN Women's Gender and Technology Report (2023) and Amnesty International's (2022) analysis of online violence, this section examines how surveillance technologies exacerbate existing gender inequalities, shaping both digital and real-world experiences of oppression.

Women and Marginalised Communities Under Heightened Surveillance

The application of surveillance technologies is not uniform; instead, it reflects and reinforces societal power hierarchies. Women, especially those from marginalised racial, ethnic, and caste groups, are subjected to disproportionate monitoring, both by state actors and private entities (Amnesty International, 2022).

- **State Surveillance and Gendered Policing:**

  Governments worldwide have weaponised digital surveillance against female activists, journalists, and human rights defenders. In many authoritarian regimes, feminist organisers are closely monitored, with their digital communications being intercepted to suppress dissent. According to UN Women (2023), women advocating for reproductive rights and gender equality in countries like Iran, India, and Saudi

Arabia face targeted digital repression, often through spyware and hacking attempts.

- **Predictive Policing and racialised Gender Bias:**

  AI-driven predictive policing disproportionately impacts women of colour, Dalits, and Indigenous communities. These surveillance tools, which rely on historical crime data, often misidentify marginalised women as criminal threats, leading to over-policing and criminalisation of survival strategies, such as sex work (Eubanks, 2018).

- **Workplace Surveillance and Gendered Labour Control:**

  Women in informal labour sectors and gig economies face intense digital surveillance through productivity-tracking software, biometric verification, and AI-based performance evaluations (Adams-Prassl, 2021). Studies show that these surveillance tools frequently penalise women for caregiving responsibilities, reinforcing workplace discrimination. This heightened scrutiny demonstrates that digital surveillance is not just about privacy invasion; it is a mechanism of social control that regulates and restricts women's agency in digital and physical spaces.

AI-Driven Discrimination, Cyberstalking, and Doxxing as Gendered Threats

Artificial intelligence (AI) and digital platforms have automated and amplified existing gendered threats, making women more vulnerable to cyberstalking, doxxing, and algorithmic bias.

AI-Driven Discrimination

AI systems are often trained on biased datasets, reflecting historical gender and racial disparities. This has resulted in:

- Discriminatory Hiring Algorithms: AI-based hiring tools have been found to downgrade resumes from women applicants in STEM fields, as seen in Amazon's AI recruitment model, which was scrapped after it was found to systematically favour male candidates (Dastin, 2022).
- Algorithmic Censorship: Social media moderation systems disproportionately flag feminist content as "harmful" while allowing misogynistic and violent speech to circulate (Noble, 2018).
- Facial Recognition Bias: Studies by Buolamwini and Gebru (2018) found that facial recognition software misidentifies Black women at higher rates, leading to discriminatory profiling in public spaces.

Cyberstalking and Digital Harassment

- The digitization of personal information has made women more susceptible to cyberstalking, a form of gender-based violence that exploits digital tools to exert control and fear.
- According to Amnesty International (2022), over 58% of women in major democracies report experiencing some form of cyber-harassment, including persistent tracking, unsolicited threats, and surveillance via spyware.
- The UN Women (2023) report highlights that woman in politics, media, and academia experience higher rates of online harassment, often as a deterrent to public participation.
- The rise of "stalker ware" apps used to monitor women's phones without consent—has escalated cases of intimate partner surveillance, with over 30% of domestic abuse victims reporting digital stalking (Dragiewicz et al., 2018).

Doxxing and Public Exposure of Women's Private Information

- Doxxing the malicious release of private information, such as addresses, phone numbers, and personal records has become a common tool for gendered digital violence.
- Women journalists and activists are frequent targets. UNESCO (2020; 2021) reports that 73% of women journalists globally have faced doxxing and coordinated digital harassment campaigns, often leading to real-world threats.

- Revenge Porn and Non-Consensual Image Sharing: The rise of deepfake pornography and AI-generated non-consensual images has increased public humiliation and blackmailing of women (Citron & Chesney, 2019). The Sulli Deals and Bulli Bai cases in India exemplify how Muslim women were specifically targeted in digitally orchestrated misogynistic auctions.
- These AI-driven and cyber-enabled threats underscore the need for gender-sensitive regulations, stronger digital rights protections, and greater corporate accountability in mitigating online violence.

Case Studies from Reports on Gendered Digital Surveillance

- **Case Study 1: UN Women's Gender and Technology Report (2023)**

  This report provides comprehensive data on how gender intersects with digital surveillance, emphasising the disproportionate impact on women in the Global South. Key findings include:

  - Women's Data Vulnerability: Women's online activity is closely monitored in authoritarian states, often leading to legal repercussions for speaking about gender-based violence.
  - Reproductive Surveillance: Data from health-tracking apps has been weaponised to police reproductive rights, particularly in restrictive legal environments.
  - AI-Based Misinformation: Women, especially those in politics, are more likely to be victims of deepfake technology, spreading false and sexually explicit content to discredit them.

- **Case Study 2: Amnesty International (2022) Report on Online Violence Against Women. Amnesty International's research highlights:**

  - Over 50% of women report self-censoring online due to fear of harassment.
  - Women of colour, LGBTQ+ individuals, and religious minorities face more severe and persistent forms of online violence.
  - Lack of legal recourse: Digital platforms and law enforcement fail to address online violence, leaving women vulnerable to continuous abuse.

These findings reinforce the urgent need for feminist digital policies, including stronger cybersecurity laws, corporate accountability measures, and victim-centred support systems.

THE POLITICAL ECONOMY OF SURVEILLANCE

The political economy of surveillance refers to the ways in which states and corporations collect, control, and monetise personal data, often under the guise of security, efficiency, and consumer convenience. In a data-driven economy, surveillance is not just a technological phenomenon it is an economic and political tool that reinforces existing power hierarchies (Zuboff, 2019). The increasing convergence of state surveillance and corporate data collection has created a landscape where privacy is systematically eroded, disproportionately affecting women and marginalised communities. This section explores the corporate-state nexus in digital surveillance, the gendered consequences of predictive policing and facial recognition technologies, and the differentiated impacts of surveillance in the Global North and Global South.

- **Corporate and State Control Over Personal Data**

  Surveillance today operates through a symbiotic relationship between states and corporations. While states justify surveillance on the grounds of national security, governance, and crime prevention, corporations collect user data under the pretext of personalisation and consumer insights. In both cases, women and marginalised communities are disproportionately targeted as surveillance subjects.

- **Corporate Surveillance: The Rise of Data Extraction Capitalism**

  Shoshana Zuboff (2019) defines surveillance capitalism as a system in which corporations extract behavioural surplus data from users to predict and manipulate human behaviour. In this model, personal data is transformed into a commodity for economic and political control.

- **Big Tech's Role in Gendered Surveillance:**

  Corporate giants like Google, Meta (Facebook), Amazon, and TikTok collect vast amounts of personal data, including location, communication history, purchasing patterns, and biometric information. Studies show that women are disproportionately surveilled through targeted advertising, reproductive health tracking, and AI-driven consumer profiling (Noble, 2018).

- **Gendered Data Exploitation in Reproductive Health Apps:**

  Apps such as Flo, Clue, and Ovia, which track menstrual cycles, fertility, and pregnancy-related data, have been found selling user data to third parties without consent (Mozilla Foundation, 2022). In the post-Roe v. Wade era, the U.S. has witnessed increased state interest in accessing reproductive health data for law enforcement purposes, raising concerns about women's bodily autonomy in digital spaces.

Workplace Surveillance and Digital Labor Exploitation:

Women in precarious labour sectors, particularly gig work, face continuous surveillance through algorithmic tracking and productivity monitoring software, reinforcing workplace inequalities (Adams-Prassl, 2021). AI-driven management tools disproportionately penalize female workers for caregiving responsibilities, limiting their economic mobility and reinforcing structural disadvantages (Gray & Suri, 2019). Similarly, state surveillance has expanded into digital authoritarianism, disproportionately impacting gendered and marginalised identities. Governments worldwide deploy mass biometric data collection, such as Aadhaar in India and China's Social Credit System, to monitor populations, while predictive policing and algorithmic crime forecasting often reflect and exacerbate existing biases. The online censorship of feminist and activism further restricts marginalised voices, and the use of spyware against women journalists and activists highlights the explicitly gendered nature of state surveillance. Across different regions, digital tools are weaponized to regulate and suppress women's movements and freedoms, reinforcing patriarchal control in both public and private spaces.

Gendered Implications of Predictive Policing and Facial Recognition Technologies

Predictive policing and facial recognition technologies (FRTs) are increasingly deployed by law enforcement agencies worldwide. These AI-driven tools, however, are not neutral or objective; they are shaped by historically biased data that disproportionately misclassifies and over-polices marginalised communities, particularly Black women, Dalit women, and Indigenous communities (Buolamwini & Gebru, 2018).

- **The Problem of Predictive Policing**

  Predictive policing algorithms claim to anticipate crime patterns based on historical data, but research reveals significant biases that disproportionately impact marginalised women. Women in low-income neighbourhoods are often flagged as "high-risk", resulting in increased police harassment and criminalisation (Eubanks, 2018). Additionally, sex workers and transgender women are frequently misclassified as criminal threats, reinforcing discriminatory law enforcement practices that deepen systemic inequalities (Keyes, 2018). Biases also extend to domestic violence risk assessments, where AI-driven tools used by police departments fail to prioritise survivors' safety. These flawed algorithms can lead to wrongful arrests or inadequate protection measures for women, undermining justice and support for victims of domestic violence (Richardson et al., 2019). Instead of fostering public safety, predictive policing reinforces existing prejudices, disproportionately targeting vulnerable groups while failing to address the root causes of crime and violence.

- **Facial Recognition: Gender and Racial Bias**

  Facial recognition technologies (FRTs) have been widely criticised for their inaccuracy and bias, particularly against women and people of colour. A 2018 MIT study revealed that commercial facial recognition systems misidentified Black women at rates of up to 34%, compared to less than 1% for white men (Buolamwini & Gebru, 2018). These biases have serious consequences, as women's faces are more likely to be misclassified in law enforcement databases, increasing the risk of wrongful arrests and legal discrimination (Garvie, 2019). Moreover, feminist activists and protesters face heightened risks, as FRT-enabled police surveillance is used to track and suppress political dissent, discouraging women's participation in activism (Amnesty International, 2022). Despite growing evidence of these harms, governments and corporations continue

to expand the use of facial recognition, reinforcing gendered surveillance and digital discrimination while failing to address its deeply ingrained biases.

The Global North vs. Global South: Authoritarian Surveillance and Its Gendered Consequences

The effects of digital surveillance are not uniform across the globe; they are deeply shaped by geopolitical contexts, with women in the Global South experiencing heightened vulnerabilities due to weaker legal protections, authoritarian policies, and neocolonial data extraction practices. In the Global North, corporate surveillance operates within a framework of digital capitalism, where women's personal data is primarily commodified for profit through advertising, AI profiling, and targeted content (Noble, 2018). Although laws like the General Data Protection Regulation (GDPR) offer some safeguards, gendered biases embedded in AI and social media platforms continue to pose challenges. In contrast, the Global South faces a more repressive form of digital surveillance, where both corporate and state-controlled mechanisms intensify the monitoring of women. In countries such as Saudi Arabia, China, and India, surveillance is weaponised to suppress feminist activism, criminalise online dissent, and restrict reproductive autonomy (UN Women, 2023). Furthermore, data colonialism (Couldry & Mejias, 2019) exacerbates these inequalities, as corporations from the Global North extract vast amounts of data from populations in the Global South without ethical oversight. This dynamic fosters digital dependency, leaving women in low-income countries subjected to pervasive surveillance without meaningful consent or control over their personal information.

Whereas in addition to the Indian context, it is critical to examine how gendered digital surveillance manifests across other regions of the Global South, particularly in Latin America and Sub-Saharan Africa. In Uganda, feminist activists and opposition leaders have increasingly become targets of state-sponsored digital surveillance during protests against gender-based violence and political repression. Reports from digital rights organisations, such as *Access Now* and *CIPESA*(Collaboration on International ICT Policy for East and Southern Africa), highlight the use of spyware, social media monitoring, and digital blacklisting to intimidate and silence women-led movements. During the 2021 Ugandan general elections, women activists reported extensive surveillance of their online communications, leading to arrests and detentions based on their social media posts. This surveillance has had a chilling effect on women's civic participation and digital expression, reinforcing authoritarian control under the guise of "cybersecurity". Similarly, in Brazil, Afro-Brazilian women, particularly those in political or journalistic roles, face coordinated digital harassment campaigns that often deploy tools like deepfakes, doxxing, and racist cyberbullying to suppress their visibility and credibility. The 2018 municipal election in Rio de Janeiro, for instance, witnessed a spike in online threats and deepfake pornography targeting Black women candidates, including threats of sexual violence and assassinations. This digital violence is not merely incidental but is embedded within the broader context of racialised and gendered power hierarchies, functioning as a deterrent to Black women's political participation. As highlighted by valente (2023), the intersection of race, gender, and political dissent makes Afro-Brazilian women uniquely vulnerable to digitally facilitated gender-based violence. These cases illustrate how digital technologies, when left unregulated or deployed by oppressive state and social forces, are weaponised to reinforce patriarchal, racial, and colonial control. The experiences of women in Uganda and Brazil reflect broader patterns of data colonialism, where surveillance regimes disproportionately target marginalised women in the Global South, exacerbating both digital and offline inequalities.

FEMINIST CRITIQUES OF SURVEILLANCE

Surveillance is often presented as a neutral technology designed for security, efficiency, and governance. However, feminist scholars argue that surveillance is deeply gendered, racialised, and classed, disproportionately targeting women and marginalised communities (Dubrofsky & Magnet, 2015; Noble, 2018). Feminist critiques of surveillance highlight how surveillance technologies reinforce existing power structures, exacerbating gender and social inequalities rather than mitigating them. Surveillance is not merely a tool for monitoring but also an instrument of patriarchal control, used to scrutinise, police, and discipline marginalised individuals, particularly women. Scholars such as Dubrofsky and Magnet (2015) argue that digital surveillance functions as an extension of societal control, dictating acceptable behaviour and punishing deviations from patriarchal norms. Historically, feminist theories have traced surveillance's roots to patriarchal oversight of women's bodies and choices, from state-imposed reproductive controls to the policing of public and private conduct (Bartky, 1990). Today, digital technologies have intensified these practices, making surveillance more insidious and pervasive.

One key aspect of gendered surveillance is the monitoring and policing of women's digital presence. Social media platforms disproportionately censor content related to women's sexuality, feminism, and body positivity while permitting misogynistic and violent content to thrive (Gillespie, 2018). Female journalists and activists face heightened online surveillance, often leading to harassment and targeted threats, as seen in cases from India and the Middle East (Amnesty International, 2022). Additionally, state surveillance extends to reproductive choices, as seen in post-Roe v. Wade America, where authorities could potentially use digital data from period-tracking apps, search histories, and location tracking to criminalise abortion seekers (Mozilla Foundation, 2022). This gendered data exploitation is further exacerbated by AI-driven surveillance technologies, which misclassify women and gender-diverse individuals, resulting in false identifications and over-policing (Buolamwini & Gebru, 2018).

Despite increasing awareness of gender-based digital surveillance, most global privacy and security policies remain gender-blind. Existing frameworks, such as the EU General Data Protection Regulation (GDPR) and India's Digital Personal Data Protection Act (2023), emphasise individual consent and data security but fail to address gender-specific risks. Cyberstalking, doxxing, and deepfake pornography disproportionately impact women and gender-diverse individuals, yet these acts are not consistently classified as serious crimes under digital policies (Citron & Chesney, 2019). AI-driven hiring algorithms have been found to discriminate against women, as seen in Amazon's 2018 AI recruitment tool, which penalised resumes containing words like "women's studies" (Dastin, 2022). The lack of regulation on corporate data exploitation also disproportionately affects women, as big tech companies collect and sell their digital data without explicit consent, often exposing them to increased surveillance and harassment (Mozilla Foundation, 2022).

Feminist critiques emphasise that surveillance disproportionately affects marginalised communities, particularly LGBTQ+ individuals and women from racialised or lower-caste backgrounds. Intersectionality (Crenshaw, 1989) highlights that experiences of surveillance are shaped by overlapping axes of oppression, such as race, class, and sexuality. LGBTQ+ individuals face heightened digital surveillance, especially in countries where same-sex relationships are criminalised, with governments using AI-based policing and social media tracking to monitor and arrest them. Similarly, facial recognition technology has been shown to misidentify Black women at disproportionately high rates, leading to increased scrutiny and wrongful accusations (Buolamwini & Gebru, 2018). In India, Dalit and Muslim women activists have been subjected to heightened state surveillance, with AI-driven social media monitoring used to target and arrest them (Amnesty International, 2022). These patterns of digital surveillance reinforce systemic inequalities, silencing marginalised voices and restricting their access to digital spaces.

Addressing gendered surveillance requires a feminist-informed approach to data governance, which acknowledges and mitigates these inequalities. Feminist scholars argue that surveillance capitalism (Zuboff, 2019) and algorithmic bias (Buolamwini & Gebru, 2018) disproportionately impact women and marginalised communities, necessitating the implementation of inclusive data policies. A feminist digital rights framework should advocate for consent and autonomy in data collection, emphasise data minimisation to prevent mass surveillance, and address structural inequalities in global data governance (Couldry & Mejias, 2019). Legal and technological reforms must also recognise technology-facilitated gender-based violence (TFGBV) as a serious crime and regulate AI-driven discrimination. Without such interventions, surveillance technologies will continue to reinforce patriarchal, racialised, and class-based power structures rather than fostering a more equitable digital landscape.

CONCLUSION AND RECOMMENDATIONS

The expansion of digital technologies has led to unprecedented levels of surveillance, raising serious concerns about privacy, autonomy, and human rights. This paper has examined how gendered surveillance disproportionately affects women, LGBTQ+ individuals, and marginalised communities, exacerbating existing social inequalities. Surveillance capitalism, as theorised by Zuboff (2019), enables corporations and states to extract and exploit personal data—often without consent—while algorithmic governance, as discussed by Noble (2018), reinforces structural discrimination through biased AI systems, facial recognition, and predictive policing. These systems transform digital infrastructures into mechanisms of control that deepen marginalisation rather than protect users. A critical takeaway from this study is the failure of existing digital governance models to account for gender-specific vulnerabilities. While frameworks such as the EU General Data Protection Regulation (GDPR) and India's Digital Personal Data Protection Act (2023) introduce

privacy safeguards, they largely ignore the gendered and intersectional nature of digital harms. Technology-facilitated gender-based violence (TFGBV), including doxxing, cyberstalking, and deepfake pornography, remains inconsistently addressed in legal and regulatory frameworks, leaving victims with limited avenues for redress (Citron & Chesney, 2019). Moreover, AI systems frequently misidentify and misclassify marginalised individuals, as Buolamwini and Gebru (2018) demonstrated in their study on facial recognition bias. In the Global South, digital surveillance is further weaponised by authoritarian regimes to silence feminist activists, journalists, and LGBTQ+ individuals (Rahman, 2023), underscoring the need for feminist digital governance frameworks rooted in justice, inclusion, and intersectionality.

Intersectionality is central to understanding how surveillance operates along multiple axes of oppression. Women and gender-diverse individuals from Dalit, Muslim, Black, Indigenous, and LGBTQ+ communities face compound risks in digital spaces due to overlapping systems of caste, race, class, and sexuality. A feminist approach to digital governance must account for these intersecting forms of discrimination and prioritise collective privacy rights and participatory data justice models.

Legal Reforms

To address these challenges, legal reforms must explicitly recognise and criminalise TFGBV. Cybercrime laws should be updated to include emerging digital harms such as doxxing, non-consensual image sharing, and algorithmic discrimination (Citron & Chesney, 2019). Governments should require Big Tech companies to conduct intersectional impact assessments for AI-driven systems, particularly those used in law enforcement, hiring, and content moderation (Mozilla Foundation, 2022). Privacy laws must also shift from an individualistic model of consent to collective, community-based data protection frameworks that acknowledge the differential risks faced by marginalised groups (Nissenbaum, 2010).

Technological Interventions

Technological solutions must be grounded in ethical design and intersectional representation. AI systems should be developed using inclusive, bias-aware datasets, with ongoing audits conducted by independent bodies. Government agencies and research institutions must fund transparency-driven evaluations of AI tools used in critical sectors such as policing, border control, and welfare administration. At the platform level, encryption mechanisms, decentralised identity systems, and privacy-preserving architectures should be adopted to minimise the risks of surveillance (UN Women, 2023). Open-source, community-led digital safety tools can offer grassroots protection and promote autonomy in surveillance-heavy contexts.

Education and Capacity Building

Beyond structural reforms, education and capacity building are vital for resistance. Women's under-representation in cybersecurity – just 26% globally (Morgan, 2022) – highlights the need for gender-inclusive training initiatives. Educational programmes must empower individuals, especially young women and gender-diverse persons, with digital literacy, privacy rights knowledge, and online safety strategies. Feminist and decolonial data governance movements must be integrated into policy discussions to confront Western-centric digital models that often exclude or exploit communities in the Global South (Couldry & Mejias, 2019; Gurumurthy & Chami, 2021).

Towards Collective Action

Challenging surveillance capitalism and algorithmic oppression requires collective action at multiple levels. Policymakers must be held accountable for enforcing gender-sensitive digital rights frameworks, while civil society, feminist collectives, and digital rights organisations must mobilise for structural change. Global solidarity is essential to confront the authoritarian misuse of digital tools and to reframe privacy not as a luxury but as a fundamental right grounded in dignity, autonomy, and equality. Decolonising digital governance begins by centring the voices of historically excluded populations and ensuring that they are integral to shaping ethical, equitable, and feminist technologies.

Policy Recommendations

- **Mandate intersectional impact assessments** of AI systems across public and private sectors.
- **Criminalise technology-facilitated gender-based violence**, including doxxing, deepfake abuse, and

cyberstalking.

- **Develop collective consent frameworks** to replace individualistic data protection models.
- **Fund grassroots digital literacy programmes**, prioritising the participation of women and marginalised groups.
- **Support South–South collaborations** to create feminist, decolonial alternatives to Western-centric surveillance regimes.

In conclusion, the future of digital governance must be inclusive, intersectional, and feminist. Without deliberate and multidimensional interventions, digital surveillance will continue to reinforce structural inequalities, expand the gender digital divide, and erode democratic freedoms. Technology should serve as a tool of empowerment, not oppression. The pursuit of digital justice is a shared responsibility that demands solidarity, sustained advocacy, and transformative policymaking to build safer and more equitable digital futures for all.

DECLARATIONS

Acknowledgement

The authors would like to thank colleagues and scholars in the field of digital rights, feminist studies, and surveillance research whose insights and literature have significantly shaped the conceptual development of this paper. I also acknowledge the Indian Council of Social Science Research (ICSSR), Ministry of Education, Government of India, New Delhi, for awarding a Doctoral Fellowship that supported this research. The views expressed in this paper are those of the authors alone.

Authors' Contribution

Conceptualization, M.I. and N.M.; methodology, M.I.; validation, M.I., N.M., and S.S.; formal analysis, M.I.; investigation, M.I.; resources, M.I.; writing original draft preparation, M.I.; writing review and editing, M.I., N.M., and S.S.; visualization, M.I.; supervision, N.M.; project administration, M.I.; funding acquisition, N.M. All authors have read and agreed to the published version of the manuscript.

Funding Information

I am deeply honoured to have been awarded a Doctoral Fellowship by the Indian Council of Social Science Research (ICSSR). This publication is an outcome of ICSSR-sponsored doctoral research. However, I bear sole responsibility for the information presented, the views expressed, and the findings of this study. I am sincerely grateful to the ICSSR, Ministry of Education, Government of India, New Delhi, for their invaluable financial support, which made this work possible. This research was supported by the Indian Council of Social Science Research (ICSSR), Ministry of Education, Government of India, under its Doctoral Fellowship scheme.

Availability of Data and Materials

Not applicable. This research is a conceptual paper and does not rely on empirical data. All arguments are grounded in published literature, theoretical frameworks, and secondary sources cited within the manuscript.

Declaration of Conflict

The authors declare no conflict of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript, or in the decision to publish the results.

Clinical Trial Number

Not applicable.

Human Ethics and Consent to Participate

Not applicable. This paper is based on conceptual and theoretical analysis and does not involve human

participants or primary data collectiol.

REFERENCES

Adams-Prassl, J. (2021). *Humans as a service: The promise and perils of work in the gig economy*. Oxford University Press.

Amnesty International. (2022). *We are being watched: Facial recognition technology and the threat to our rights*. Amnesty International.

Banet-Weiser, S. (2018). *Empowered: Popular feminism and popular misogyny*. Duke University Press.

Bartky, S. L. (1990). *Femininity and domination: Studies in the phenomenology of oppression*. Routledge.

Bivens, R., & Haimson, O. L. (2016). Baking gender into social media design: How platforms shape categories for users and advertisers. *Social Media + Society, 2*(4). https://doi.org/10.1177/2056305116672486

Buolamwini, J., & Gebru, T. (2018). Gender shades: Intersectional accuracy disparities in commercial gender classification. In S. A. Friedler & C. Wilson (Eds.), *Proceedings of the Conference on Fairness, Accountability, and Transparency* (*Proceedings of Machine Learning Research*, Vol. 81, pp. 1–15). PMLR. https://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf

Citron, D. K., & Chesney, R. (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. *California Law Review, 107*(6), 1753–1819. https://scholarship.law.bu.edu/faculty_scholarship/640

Crenshaw, K. (1989). Demarginalizing the intersection of race and sex: A Black feminist critique of antidiscrimination doctrine, feminist theory and antiracist politics. *University of Chicago Legal Forum*, 139–167. http://scholarship.law.columbia.edu/cgi/viewcontent.cgi?article=4013&context=faculty_scholarship

Chun, W. H. K. (2006). *Control and freedom: Power and paranoia in the age of fiber optics*. MIT Press.

Couldry, N., & Mejias, U. A. (2019). *The costs of connection: How data is colonizing human life and appropriating it for capitalism*. Stanford University Press.

Dastin, J. (2022). Amazon scraps secret AI recruiting tool that showed bias against women. In *Ethics of data and analytics* (1st ed., p. 4). Auerbach Publications. https://doi.org/10.1201/9781003278290

Dragiewicz, M., Burgess, J., Matamoros-Fernández, A., Salter, M., Suzor, N. P., Woodlock, D., & Harris, B. (2018). Technology facilitated coercive control: Domestic violence and the competing roles of digital media platforms. *Feminist Media Studies, 18*(4), 609–625. https://doi.org/10.1080/14680777.2018.1447341

Dubrofsky, R. E., & Magnet, S. A. (Eds.). (2015). *Feminist surveillance studies*. Duke University Press. https://doi.org/10.1215/9780822375463

Eubanks, V. (2018). *Automating inequality: How high-tech tools profile, police, and punish the poor*. St. Martin's Press.

Foucault, M. (1977). *Discipline and punish: The birth of the prison* (A. Sheridan, Trans.). Pantheon Books.

Gandy, O. H. (1993). *The panoptic sort: A political economy of personal information*. Westview Press.

Garvie, C. (2019). *Garbage in, gospel out: Facial recognition and policing bias*. Georgetown Law Center on Privacy & Technology.

Gillespie, T. (2018). *Custodians of the Internet: Platforms, content moderation, and the hidden decisions that shape social media*. Yale University Press. https://doi.org/10.12987/9780300235029

Gray, M. L., & Suri, S. (2019). *Ghost work: How to stop Silicon Valley from building a new global underclass*. Houghton Mifflin Harcourt.

Gurumurthy, A., & Chami, N. (2021). Towards a global digital constitutionalism: A radical new agenda for

UN75. *Development, 64*(1–2), 29–38. https://doi.org/10.1057/s41301-021-00287-z

Keyes, O. (2018). The misgendering machines: Trans/HCI implications of automatic gender recognition. *Proceedings of the ACM on Human–Computer Interaction, 2*(CSCW), Article 88, 1–22. https://doi.org/10.1145/3274357

Lambrecht, A., & Tucker, C. (2019). Algorithmic bias? An empirical study of apparent gender-based discrimination in the display of STEM career ads. *Management Science, 65*(7), 2966–2981. https://doi.org/10.1287/mnsc.2018.3093

Morgan, S. (2022, August 10). *Boardroom cybersecurity 2022 report: Cybercrime facts, figures, predictions and statistics* [Press release]. Cybersecurity Ventures. https://cybersecurityventures.com/boardroom-cybersecurity-report/

Mozilla Foundation. (2022). *Privacy not included: Guide to connected products*.

Nissenbaum, H. (2010). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press.

Noble, S. U. (2018). *Algorithms of oppression: How search engines reinforce racism*. NYU Press.

Richardson, R., Schultz, J. M., & Crawford, K. (2019). Dirty data, bad predictions: How civil rights violations impact predictive policing. *New York University Law Review, 94*(2), 15–55. https://nyulawreview.org/wp-content/uploads/2019/04/NYULawReview-94-Richardson_etal-FIN.pdf

UNESCO. (2021a). *The chilling: Global trends in online violence against women journalists*. Retrieved May 15, 2025, from https://unesdoc.unesco.org/ark:/48223/pf0000377223

UNESCO. (2020). *Online violence against women journalists: A global snapshot of incidence and impacts*. Retrieved May 15, 2025, from https://unesdoc.unesco.org/ark:/48223/pf0000375136

UN Women. (2021). *Violence against women in the online space: Insights from a multi-country study in the Arab States*. Retrieved May 15, 2025, from https://arabstates.unwomen.org/en/digital-library/publications/2021/11/violence-against-women-in-the-online-space

UN Women. (2023). *Progress on the sustainable development goals: The gender snapshot 2023*. https://www.unwomen.org/sites/default/files/2023-09/progress-on-the-sustainable-development-goals-the-gender-snapshot-2023-en.pdf

Valente, M. (2023). *Online gender-based violence in Brazil: New data insights* (Supporting a Safer Internet Paper No. 4). Centre for International Governance Innovation. https://www.cigionline.org/static/documents/SaferInternet_Paper_no_4.pdf

Van Dijck, J. (2014). Datafication, dataism and dataveillance: Big data between scientific paradigm and ideology. *Surveillance & Society, 12*(2), 197–208. https://doi.org/10.24908/ss.v12i2.4776

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. PublicAffairs.