Journal of legal and social studies

Issn: 2507-7333

Eissn: 2676-1742

The Digital Society and New Mechanisms of Social Control: When the Public Becomes the Censor

Samia boukehil*

University of Mohamed Seddik Ben Yahia - Jijel, Algeria,
samia.boukehil@univ-jijel.dz

Date of send: 01/03/2026	date of acceptance: 01/05/2026	Date of Publication: 01/06/2026

***Corresponding author**

Abstract :
This paper offers a critical reading of how contemporary communication environments contribute to shaping mechanisms of social regulation and authority within society. Employing a semi-systematic literature review methodology based on the PRISMA framework, the study analyzes 24 peer-reviewed articles from the Scopus database (2020-2026) to examine social media practices and their repercussions on the public sphere. The research seeks to clarify how technological transformations impose a form of technological determinism in constructing social structures and forming both social and cybernetic entities. The findings reveal three primary patterns: (1) digital platforms have evolved into quasi-public institutions exercising sovereign powers through algorithmic governance; (2) the Digital Panopticon model transforms users into simultaneous guards and prisoners, where mutual surveillance normalizes disciplinary behaviors; and (3) participatory surveillance and cancel culture represent new forms of social control that challenge traditional legal frameworks. The study concludes that surveillance in digital society has shifted from centralized top-down monitoring to a decentralized, liquid system where surveillance roles are distributed among the public, creating unprecedented challenges for privacy and individual liberty.

Keywords: Digital Society; Social Control; Participatory Surveillance; Algorithmic Governance.

1. Introduction

The twenty-first century is characterized by intensive human reliance on information and communication technologies, where the dynamic development of digital media has contributed to fundamental changes in social interaction and public opinion formation processes. Digital platforms are no longer mere communication tools; they have become fundamental infrastructure enabling individuals to participate in economic and social life, just as railways and roads did in the past. Through sophisticated algorithms based on big data, these platforms shape how users organize digital resources to build social relationships and conduct market transactions.

The problem of this article crystallizes in the fading of traditional boundaries between the public and private sectors under the hegemony of platform capitalism. This transformation raises fundamental questions about the legitimacy of the authority exercised by platforms in setting standards and imposing digital sanctions, and the adequacy of traditional regulatory frameworks to confront surveillance capitalism[1].

That transforms human behavior into economic value. To address this problem, the article relies on the qualitative literature review methodology to analyze contemporary academic production.

Research Hypotheses

Hypothesis 1: Digital Platforms as Infrastructure for Quasi-Public Regulation. This hypothesis starts from the idea that digital platforms are no longer mere commercial companies, but have transformed into quasi-public institutions that manage digital space and perform functions that were the exclusive preserve of the state, such as organizing access to basic services and information.

Hypothesis 2: Algorithmic Fragmentation and Herd Censorship Guidance. This hypothesis considers that algorithmic content personalization not only isolates individuals within filter bubbles[2], but also works as a technical mechanism for fragmenting public opinion and directing public attention toward specific issues that increase the intensity of biases.

Hypothesis 3: The Digital Panopticon and Normalization of Self-Discipline. This hypothesis focuses on the behavioral aspect, where contemporary platforms adopt the Digital Panopticon[3] model, a surveillance system that makes the individual feel under the gaze of the public and the platform together all the time.

Research Objectives

1. Analyzing the structural transformation of digital platforms into quasi-public institutions: The article aims to monitor how platforms have moved beyond their purely commercial role to become basic infrastructure managing public rights and services.

2. Investigating the role of algorithmic guidance in practicing herd censorship: The research seeks to understand how algorithms contribute to fragmenting public opinion and creating information bubbles.

3. Dissecting the Digital Panopticon model and self-discipline mechanisms: The article aims to study the shift in power balances where the user becomes both guard and prisoner simultaneously.

4. Evaluating the effectiveness of republican social control versus formal institutional control: The article seeks to examine the tension resulting from the No Viral No Justice phenomenon.

5. Proposing hybrid regulatory frameworks for digital governance: Reaching scientific perceptions that support building regulatory models that combine state oversight with public accountability principles.

THE FIRST TOPIC : Methodology

Methodology constitutes the backbone of any scientific research, as it determines the path that the researcher follows to reach reliable and verifiable results. In the context of studying The Digital Society and New Mechanisms of Social Control, methodology gains exceptional importance due to the intertwining of overlapping cognitive fields in this topic, from sociology to law through media and technology studies. The multidimensional nature of this phenomenon calls for adopting a flexible methodological approach capable of absorbing the theoretical and practical complexities posed by digital transformation in the structure of power and social control.

This study builds on the semi-systematic literature review methodology as a suitable methodological framework for the nature of the research topic. This methodology was chosen for several fundamental considerations: first, its ability to absorb the overlap between different cognitive disciplines that address the topic of digital social control; second, its flexibility in dealing with diverse sources ranging from peer-reviewed research papers, international reports, and legal studies. This methodology also allows for presenting a comprehensive critical reading of cognitive production without being bound by strict restrictions that may overlook vital aspects of the phenomenon under study.

First requirement: PRISMA Framework and Study Selection

The PRISMA Flow Diagram (Preferred Reporting Items for Systematic Reviews and Meta-Analyses)[4] is an approved methodological tool in academic research, especially in systematic reviews and meta-analyses. This diagram was designed to visually display the path of study selection, starting from the initial search stage until reaching the final studies that were included in the analysis.

Inclusion Criteria:

- Studies published in Scopus-indexed journals, in English from 2020-2026
- Studies addressing: Digital society, Social control, Online censorship, Public censorship, Participatory surveillance, Self-censorship, Algorithmic governance, Digital governance, Social media regulation, Civic monitoring

Exclusion Criteria:

- Purely technical or experimental studies outside the field of social research
- Opinion papers and non-scientific reports
- Studies outside the specified time frame

First section : PRISMA Flow Diagram Summary

Table 1: PRISMA Flow Diagram for Study Selection

PRISMA Stage	Details of Records and Studies
Identification	145 records identified from the Scopus database through systematic search using keywords related to digital society and social control.
Screening	7 duplicates removed → 138 records remained for title and abstract screening. Subsequently, 110 records were excluded based on title and abstract assessment (not relevant to research scope).
Eligibility	28 records assessed for full-text eligibility. Of these, 6 were excluded for lack of relevance and 17 for weak relevance to the research topic.
Included	24 studies included in the final synthesis, focusing on digital surveillance, algorithmic authority, and the transformation of the public into a censor.

Table 2: Summary of Study Selection Statistics

Stage	Number of Records
Initial identification (Scopus)	145
After duplicate removal	138
After title/abstract screening	28
Studies included in final synthesis	24
Overall exclusion rate	83.4%

Source: Compiled by author

Second section :Study Analysis Findings

The analysis of the selected studies revealed several significant patterns across diverse research contexts. Table 1 presents a comprehensive summary of the 24 studies included in this review, highlighting their thematic relevance to the research questions. These studies were selected based on criteria emphasizing thematic relevance, theoretical foundations, legal timeliness, socio-psychological impact, and diversity of control actors.

Table 3: Summary of Selected Studies (n=24)

No.	Authors (Year)	Study Title	Relevance to Topic
1	Chen et al. (2026)	Attitudes Toward AI-powered Robots in Policing	Studies transformation to digital institutional control (predictive policing)
2	Wallace et al. (2026)	Algorithmic Tenancies and the Ordinal Tenant	Examines algorithmic sovereignty and economic/social control in housing
3	Beissembayeva et al. (2026)	Algorithmic Linguistic Manipulation in Virtual Discourse	Discusses algorithmic manipulation of discourse as a control tool
4	Şot & Rappas (2026)	Displaying Devotion in Social Media: Letter TikToks	Provides Digital Panopticon model and identity performance under surveillance

5	Shajari & Agarwal (2025)	Developing a Network-centric Approach for Anomalous Behavior	Focuses on platform surveillance and anomalous behavior detection
6	Peng et al. (2026)	Modeling and Controlling Competing Opinions in Social Networks	Analyzes public opinion control mechanisms and herd formation
7	Huang & Zhou (2025)	Generative AI Outperforms Humans in Social Media Engagement	Reveals collective behavior direction through AI-generated content
8	Mittal et al. (2025)	Fostering Brand Equity Through Online Reputation Management	Discusses audience censorship through reputation management and boycotts
9	Brown-Devlin et al. (2026)	Examining the Influence of Algorithmic Message Personalization	Clarifies algorithmic personalization effects on audience perception
10	Moravec et al. (2025)	Algorithmic Personalization: A Study of Knowledge Gaps	Links algorithmic fragmentation to knowledge gaps (filter bubbles)
11	Cebollero-Salinas et al. (2025)	Socio-emotional E-competencies, Cyberaggression	Addresses cyber-violence as a tool for peer surveillance and social punishment
12	Sombatpoonsiri et al. (2026)	Ramping Up Control: Judicial Harassment and Online Smear Campaigns	Studies digital punishment and smear campaigns as alternatives to law
13	Beidollahkhani (2026)	Regulating Female Embodiment as Disciplining Citizens	Discusses body and identity control in digital space (gendered Panopticon)
14	Fu et al. (2026)	Modeling the Spatiotemporal Evolution Process of Panic-Buying	Analyzes digital herd behavior and response to informational pressures
15	Cid et al. (2026)	The Process of Reintegration: From Prison To Conditional	Links institutional control (prison) to reintegration mechanisms
16	Maben et al. (2026)	Self-starters and Lone Rangers: Approaches to AI Training	Discusses digital ethics and policies in public sector (regulatory control)
17	Tran et al. (2025)	Investigating the Relationship Between Knowledge and Media Trust	Examines media trust and surveillance awareness in governmental systems
18	Ndlovu & Mandiyanike (2025)	Gender-Based Violence 'Matters': An Analysis of Conflicting Frames	Analyzes framing of violence in media as a social control tool
19	Liu (2025)	Virtual Presence, Real Connections: Virtual Idol Fan Community	Studies virtual identity and imitation in digital communities
20	van Bruyssel et al. (2026)	From Bliss to Burden: Digital Well-being Ethnographic Inquiry	Discusses psychological burden of self-censorship and digital pressures
21	Liang (2026)	Resisting Technology Addiction with Mencius	Proposes resistance to technology addiction as a form of control resistance
22	Lutz & Büttner (2026)	'This Message was Deleted': The Psychological Consequences	Studies social anxiety and mutual surveillance in messaging apps
23	Danko et al. (2026)	Digital Regionalism: Civil Society Diplomacy	Addresses digital diplomacy and civil society as new sovereign actors
24	Rogach et al. (2025)	Artificial Intelligence in Students' Learning Activities	Discusses AI impact on educational behavior (institutional control)

Source: Compiled by author based on systematic review

The studies presented in Table 1 span multiple dimensions of digital social control. Chen et al. (2026), Wallace et al. (2026), and Maben et al. (2026) demonstrated the transformation toward digital institutional control through predictive policing, algorithmic governance in housing, and regulatory control in public sector. Beissembayeva et al. (2026), Peng et al. (2026), and Huang & Zhou (2025) highlighted algorithmic manipulation of discourse and mechanisms for controlling public opinion and collective behavior.

Şot and Rappas (2026), Beidollahkhani (2026), and Liu (2025) provided models for the Digital Panopticon and its impact on identity performance and gender discipline in digital space. Studies by Shajari and Agarwal (2025), Brown-Devlin et al. (2026), and Moravec et al. (2025) revealed platform surveillance mechanisms and algorithmic personalization effects. Mittal et al. (2025), Sombatpoonsiri et al. (2026), and Cebollero-Salinas et al. (2025) examined audience censorship, digital punishment, and cyber-aggression as tools for peer surveillance. Finally, van Bruyssel et al. (2026), Lutz & Büttner (2026), and Liang (2026) analyzed the psychological dimensions of digital surveillance and

Second requirement :Key Conceptual Framework

1. Surveillance: Processes and experiences of collecting and analyzing personal data with the aim of influencing, managing, or granting entitlements. It also refers to systematic monitoring, tracking, and collecting information about individuals, groups, or activities[5].

2. Digital Vigilantism: A process in which citizens feel collectively insulted by the actions of another citizen, and coordinate retaliatory reactions through digital platforms and mobile devices. This process includes defamation by publishing sensitive details such as home or work address (Doxing)[6].

3. Surveillance Capitalism: A new economic system that claims that human experience is free raw material that is extracted and converted into behavioral data, then processed by artificial intelligence, to produce predictive products that expect what individuals will do in the present and future [7].

4. **Panopticon**: An architectural concept designed by Jeremy Bentham to impose order through permanent vision, where those under surveillance feel that they are constantly visible without knowing when they are actually being monitored, which pushes them to self-regulate their behavior to conform to social standards[8].

Dimension	Research Gap
Institutional	Lack of frameworks explaining how platforms evolved into quasi-public institutions performing sovereign functions without public accountability
Technical	Insufficient analysis of how algorithmic personalization fragments public opinion and creates "herd surveillance" mechanisms
Social	Limited understanding of the "Digital Panopticon" where users become both guards and prisoners
Legal	Absence of protections against digital vigilantism and "mob justice" phenomena
Theoretical	Need for integrated framework connecting surveillance capitalism, participatory surveillance, and lateral surveillance

5. **Lateral/Horizontal Surveillance**: Surveillance that individuals practice against each other (peer-to-peer) instead of traditional surveillance practiced by institutions or the state from top to bottom. It is embodied in citizens use of digital tools to monitor and track their neighbors or peers[9].

6. **Participatory Surveillance:** A type of surveillance in which individuals voluntarily engage, often associated with social networking sites, where it involves social, interactive, and reciprocal aspects, where users share their data and monitor each other as part of building social bonds[10].

Third Requirement: Statement of the Research Gap

The academic literature reveals a significant gap in understanding how digital platforms, algorithmic governance, and social surveillance converge to transform the public into active agents of social control—functioning simultaneously as censors, investigators, and executors of digital punishment.

Five Key Dimensions of the Gap:

Original Contribution

This research addresses the gap by developing an integrated theoretical framework that synthesizes:

- The institutional transformation of platforms into quasi-sovereign actors
- Technical mechanisms of algorithmic control and opinion fragmentation
- Social practices of peer surveillance and cancel culture
- Legal implications of digital vigilantism competing with formal justice systems

THE SECOND TOPIC: RESULTS

Following the methodological framework established in the previous section, this chapter presents the results of the systematic analysis conducted on the selected literature and empirical data. The findings are categorized into core thematic segments, which were derived inductively through an extensive process of reading, sorting, and searching through the collected materials.

This section aims to reveal the key patterns and discursive themes regarding social control and digital interactions, moving beyond surface-level summaries to provide a detailed illustration of the findings. The presentation is structured to address the study's central research questions, providing evidence for the confirmation of hypotheses or the identification of emerging paradigm shifts within the digital society. By integrating these results, the analysis provides a comprehensive lens through which to understand the evolving dynamics of surveillance and public censorship in the Web 2.0 environment

First requirement: Theoretical and Conceptual Evaluation

Studies that addressed the concept of Panopticon are considered the cornerstone in understanding how the public transformed into a censor. The sources succeeded in updating the thought of Foucault[11] , and Deleuze [12]to fit the digital age, where social media was described as a reverse panopticon; not only does the authority monitor individuals, but individuals monitor each other. This appears clearly on platforms like TikTok, where the algorithmic self is employed to produce content that is subject to collective trials from the public (such as the West Elm Caleb case), making vision a tool for social control.

Second requirement: Technical Evaluation: Algorithmic Authority and Big Data

Studies (such as Jawad and Moravec) deepen in how algorithms work as hidden tools for control. The studies empirically proved the existence of a relationship between exposure to personalized content and the decline in self-esteem, and the formation of echo chambers,[13] that reinforce polarization. Some sources indicate the existence of a cognitive gap among the public about how these algorithms work, which weakens individuals ability to resist digital nudging[14] that directs their behavior without awareness.

Third Requirement: Legal Evaluation: Predictive Policing and AI Law

Studies on predictive policing and the European AI Act are among the most important sources that evaluated the legislative aspect. The studies show that predictive policing in smart cities represents the pinnacle of social control, where crime is predicted based on data profiling[15], The European AI Act (2024)[16] emerges as a pioneering regulatory framework that attempts to ban social profiling and mass biometric surveillance, warning against transforming society into an electronic police state.

Fourth Requirement :Social Evaluation: The Public as Censor

The studies revealed a dark side to the transformation of the public into a censor, which is cross-border digital repression[17], Digital crowds (electronic armies) are used to practice surveillance on activists and journalists, where the public becomes a tool in the hands of authorities to defame and silence opposition. Studies confirm that these mechanisms cause a state of digital anxiety and self-censorship for fear of popular trial.

THE Third Topic: Discussion

This discussion section aims to synthesize the research findings with existing theoretical frameworks to provide a comprehensive understanding of the **shifting dynamics of power and social control** in the digital era. It explores the transition from top-down disciplinary models to **horizontal and participatory surveillance**, where the public actively engages in peer-to-peer monitoring and censorship.

By critically analyzing phenomena such as **digital vigilantism** and **cancel culture**, this section highlights how 'visibility' is weaponized as a tool for social sorting and public stigmatization, often operating outside formal legal boundaries. Furthermore, the discussion investigates the role of **algorithmic governance** and **surveillance capitalism** in facilitating disciplined social control,' where personal experiences are datafied to predict and steer human behavior, ultimately transforming the digital society into a self-operating panopticon.

First requirement: Theoretical Implications

The findings illuminate a fundamental paradigm shift in how social control operates in contemporary society. The Digital Panopticon represents the structural framework for modern social control, where surveillance is no longer limited to a central tower owned by the state. Digital society has transformed into a system where every individual is both guard and prisoner simultaneously. This permanent visibility drives individuals toward self-discipline and continuous behavior modification, echoing Foucault's (1977) disciplinary mechanisms but in decentralized form. The traditional hierarchical model has given way to a "liquid" system where surveillance roles are distributed among the public (Bauman & Lyon, 2013).

Second requirement: The Paradox of Voluntary Participation

Participatory surveillance explains why the public accepts and engages in this control system. Individuals voluntarily participate in mutual data disclosure as part of social interaction. However, this "voluntary" participation often transforms the public into an extension of the eye of power (Albrechtslund, 2008). The paradox lies in the fact that democratized participation tools simultaneously function as unprecedented social control mechanisms. Users become complicit in their own surveillance, blurring the line between agency and subordination.

Third Requirement: Implications for Democratic Governance

The tension between digital mobilization and institutional legal processes raises fundamental questions about democratic governance. While digital mobilization can provide voice for marginalized groups, it carries serious risks related to mob justice and absence of legal safeguards. The presumption of innocence becomes nearly meaningless when viral condemnation precedes formal adjudication. The challenge lies in harnessing digital civic engagement's accountability potential while protecting against vigilante justice excesses and preserving institutional integrity.

CONCLUSION

In conclusion, this systematic review has synthesized an extensive body of literature to demonstrate that social control in the digital society has undergone a fundamental 'liquefaction,' transitioning from a rigid, top-down institutional model to a decentralized and participatory practice. The evidence indicates that we have entered a post-panoptic phase where the traditional central tower of control is replaced by an online-offline nexus of horizontal surveillance, effectively turning the public into a ubiquitous and self-operating censor.

This study has highlighted how visibility is now weaponized through mechanisms such as digital vigilantism and cancel culture, which function as a new breed of social punishment that bypasses formal legal frameworks and obliterates the presumption of innocence. Furthermore, the integration of algorithmic governance and surveillance capitalism has created an environment where behavioral modification is automated, forcing individuals to internalize the gaze of power and adapt their identities to meet the predictive expectations of digital platforms. Ultimately, these findings underscore that the digital society is not merely an extension of physical space but a transformative environment where the public, empowered by technology, has become the primary guardian and enforcer of social norms.

I. Results Related to Hypotheses

1. Digital Platforms as Quasi-Public Infrastructure

The study demonstrated that digital platforms have transformed from neutral technical intermediaries into "quasi-public" institutions practicing multiple regulatory functions previously exclusive to the state. This transformation represents one of the deepest shifts in societal power structures since the emergence of the modern state, as classification, punishment, and discourse regulation functions transferred from democratic institutions to private companies not subject to public accountability. This transformation manifested in three main dimensions: the regulatory dimension where algorithms classify individuals and determine their opportunities; the judicial dimension where platforms practice social sanctions alternative to law; and the legislative dimension where algorithms shape the conditions of possibility for public discourse.

2. Algorithmic Fragmentation and Herd Censorship

The study revealed that algorithms not only fragment the public sphere but also practice an advanced form of collective behavior direction that can be termed "digital herd censorship." This censorship operates through hidden mechanisms including algorithmic personalization producing isolated cognitive bubbles, automatic content generation outperforming human content in influence, and reinforcement of emotions accelerating collective behavior. Importantly, this process is not unidirectional; rather, algorithms interact with users to produce complex regulatory dynamics that are difficult to monitor and confront.

3. Digital Panopticon and Normalization of Self-Discipline

It was confirmed that digital society constitutes an evolved model of the Panopticon, where individuals practice continuous self-surveillance not due to actual monitoring but because of awareness of the possibility of monitoring at any moment. The fundamental difference from the traditional Foucauldian model is that the center is no longer a single tower but a distributed network of digital eyes including algorithms, other users, and the general public. The study revealed that this model transcends mere external discipline to produce a deeper process of "formation of the compliant self," where individuals reshape their identity according to unstated digital standards.

II. Results Related to Research Objectives

1. Structural Transformation of Digital Platforms

The structural transformation of platforms was found to have passed through three historical phases: technical mediation where the platform was a neutral tool facilitating communication; economic mediation where the platform became a marketplace for trading data and attention; and finally political mediation where the platform became a regulatory authority for discourse and behavior. This transformation redefines the concept of "public sphere" and raises fundamental questions about democratic legitimacy of platforms and their role in social life.

2. Algorithmic Guidance Mechanisms

The study revealed an integrated model of algorithmic guidance operating on four interconnected levels: the cognitive level where algorithms determine what can be known; the emotional level where feelings are directed through reinforcement of exciting content; the behavioral level where actions are shaped through recommendation and stimulation; and the social level where public opinion is formed through creating a sense of false consensus. These four levels interconnect to produce a comprehensive system of social control operating invisibly.

3. Dissecting the Digital Panopticon

The study clarified that the digital Panopticon operates through three main mechanisms: mutual surveillance where users monitor each other; exemplary punishment where cancellation cases are displayed publicly for others to heed; and voluntary normalization where individuals internalize digital standards and practice them willingly. These mechanisms emerged as producing a new form of

decentralized and distributed power, in which platforms, algorithms, and the public participate simultaneously.

4. Effectiveness of Republican Social Control

The study proved that "republican" social control practiced by the public through digital mechanisms has become more effective than formal institutional control in many aspects—it is faster in response, broader in scope, and lower in cost. However, this effectiveness comes at a high price represented in the absence of procedural guarantees: no presumption of innocence, no fair trial, no possibility of appeal, and punishment is immediate and final. This poses a fundamental problematic about justice in digital society.

III. Synthesis Results

Transformation in Social Power Structure

The study reveals a fundamental transformation in social power structure, shifting from a centralized vertical model (State → Society) to a distributed horizontal model (Platforms ↔ Algorithms ↔ Public). This transformation redefines basic concepts such as sovereignty, legitimacy, and accountability, and raises new questions about who holds the right to social regulation in digital society and what its controls are.

The Fundamental Paradox

The study reveals a fundamental paradox: the public that was subject to surveillance has become a primary actor in it, and the tools that enable expression and resistance are the same tools of surveillance. This paradox embodies the structural contradiction of digital society, where individuals cannot participate in social life without submitting to digital regulatory mechanisms.

Erosion of Public-Private Boundaries

The study shows systematic erosion of boundaries between public and private spheres, as digital platforms have become "quasi-public" spaces mixing characteristics of both. This erosion reshapes the relationship between individual and society, and raises questions about legal protection for individuals in spaces that are neither fully public nor fully private.

RECOMMENDATIONS

I. Research Recommendations

1. Developing Theoretical Frameworks

The study proposes developing an integrative theoretical framework combining Foucault's theory of power and discipline, algorithmic governance theories, and network society theories. This integrative framework can absorb the multiple complexities of digital surveillance and provide better analytical tools for understanding its dynamics. The study also proposes developing new theoretical concepts such as "algorithmic sovereignty," "distributed surveillance," and "digitally compliant self" to establish an appropriate theoretical lexicon for this emerging research field.

2. Comparative Studies

The study proposes conducting comparative research across different cultural and political contexts to understand how digital surveillance mechanisms vary between societies. Digital surveillance in democratic societies may differ fundamentally from that in authoritarian societies, and local culture may shape different responses to digital regulation. These comparative studies contribute to building a general theory applicable in multiple contexts.

3. Longitudinal Studies

The study proposes conducting longitudinal studies to track the evolution of digital surveillance mechanisms over time, especially with the accelerating development of technologies such as generative artificial intelligence and augmented reality. These studies enable understanding of evolutionary dynamics and prediction of future trends, and contribute to formulating proactive policies rather than delayed reactions.

4. Resistance and Empowerment Studies

The study proposes directing greater research attention toward studying individual and collective forms of resistance to digital surveillance. While most studies focused on regulatory mechanisms, understanding resistance mechanisms and evaluating their effectiveness is necessary for developing strategies to protect rights and freedoms in digital society.

II. Legislative and Regulatory Recommendations

1. Legal Framework for Quasi-Public Platforms

The study proposes developing a new legal framework recognizing major digital platforms as "quasi-public" institutions with special responsibilities toward society. This framework should obligate platforms to transparency in how their

algorithms work, provide accountability mechanisms when their decisions affect individuals' rights, and define procedural guarantees for users affected by platform decisions.

2. Fundamental Digital Rights

The study proposes adopting a charter of fundamental digital rights protecting individuals from algorithmic arbitrariness and guaranteeing their right to know who monitors them and how, their right to object to algorithmic decisions and request human intervention, their right to fair trial before applying any digital punishment, and their right to digital oblivion and erasure of their data. These rights constitute fundamental guarantees against arbitrariness in digital society.

3. Regulating Peer Surveillance

The study proposes developing regulatory mechanisms for digital peer surveillance protecting individuals from arbitrary defamation and cancellation. This includes legislation criminalizing organized smear campaigns, mechanisms for complaint and appeal in cases of digital punishment, and guarantees for response and correction rights. The goal is not to prevent "republican" social control but to ensure it does not become a tool for bullying and revenge.

4. Independent Oversight Bodies

The study proposes establishing independent specialized oversight bodies in digital affairs with authorities to monitor platforms, investigate complaints, and impose sanctions. These bodies must be independent from government and technology companies, and include experts from multiple fields: law, technology, sociology, and ethics.

III. Societal and Educational Recommendations

1. Critical Digital Literacy

The study proposes integrating critical digital literacy into curricula at all levels, so students learn how algorithms work and how they affect their behavior and consciousness, how to protect themselves from algorithmic manipulation, and how to practice their digital rights. This education empowers new generations to deal critically with digital technologies rather than blindly submitting to them.

2. Awareness of Self-Surveillance

The study proposes developing awareness programs helping individuals recognize the self-surveillance mechanisms they practice in digital space. This

awareness is the first step toward liberation from digital social pressure, as individuals who realize how they exercise surveillance on themselves can consciously decide what they want to retain and what they want to change.

3. Strengthening Digital Civil Society

The study proposes supporting and strengthening civil society organizations working to protect digital rights and confront algorithmic arbitrariness. These organizations enable individuals to organize collectively to confront platform power, provide legal and technical support to those affected, and exert pressure on policymakers in favor of digital rights.

4. Comprehensive Societal Dialogue

The study proposes opening comprehensive societal dialogue about the future of digital surveillance including all stakeholders: governments, platforms, civil society, academics, and the general public. This dialogue must address fundamental questions: What are acceptable limits for digital surveillance? Who holds the right to impose it? What guarantees are necessary? How do we balance protection and freedoms?

IV. Practical Recommendations for Individuals

1. Personal Protection Strategies

The study proposes adopting practical strategies for self-protection in digital space including: limiting excessive personal sharing, using available privacy tools, critical thinking before sharing, and avoiding impulsive responses to exciting content. These strategies do not replace collective solutions but provide primary protection for individuals.

2. Building Alternative Communities

The study proposes supporting the building of alternative digital communities adopting values different from those prevailing in major platforms. These communities can provide safer spaces more respectful of privacy, and represent alternative models for digital social organization.

3. Active Participation in Rights Defense

The study proposes encouraging individuals to actively participate in defending their digital rights through: joining relevant civil society organizations, participating in public dialogues about digital policies, and supporting legislative initiatives to protect digital rights.

Closing

This research reveals a profound transformation in the structure of contemporary social power, where digital platforms, algorithms, and the public have become partners in the social regulation process. This transformation carries opportunities for enhancing democratic participation, but it also carries significant risks represented in erosion of privacy, absence of accountability, and coercive self-surveillance.

The greatest challenge facing contemporary societies is not only in understanding digital surveillance mechanisms, but in developing effective responses that balance necessary protection and fundamental freedoms, between regulatory efficiency and justice guarantees, between technical innovation and human values. This requires collective effort including researchers, legislators, civil society, and individuals, and also requires genuine political will to set limits on platform power and protect human dignity in the digital age.

References

[1] Zuboff, S. (2019). The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. PublicAffairs,p524 .
[2] Pariser, E. (2011). The Filter Bubble: What the Internet Is Hiding from You. Penguin Press,p11.
[3] Foucault, M. (1977). Discipline and Punish: The Birth of the Prison. Trans. A. Sheridan. Pantheon Books,p
[4] Page, M. J., McKenzie, J. E., Bossuyt, P. M., et al. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. BMJ, 372, n71.p p 200-217.
[5] Books: David Lyon, The Culture of Surveillance: Watching as a Way of Life, John Wiley & Sons, 2018,P. 6.
[6] Nocun, K., & Pace, M. (2021). Digital vigilantism: A systematic literature review. Internet Policy Review, 10(4),p55.
[7] Zuboff, S. (2015). Big Other: Surveillance capitalism and the prospects of an information civilization. Journal of Information Technology, 30(1), 75-89,p75.
[8] Bentham, J. (1791). Panopticon; or, The Inspection House. T. Payne,p43.
[9] Andrejevic, M. (2005). The work of watching one another: Lateral surveillance, risk, and governance. Surveillance & Society, 2(4), 479-497.p488.
[10] Albrechtslund, A. (2008). Online social networking as participatory surveillance. First Monday, 13(3),p7.
[11] Foucault, M. (1977). Discipline and Punish: The Birth of the Prison. Trans. A. Sheridan. Pantheon Books,p217.
[12] Deleuze, G. (1992). Postscript on the Societies of Control. October, 59,p 3-7.
[13] Sunstein, C. R. (2001). Echo Chambers: Bush v. Gore, Impeachment, and Beyond. Princeton University Press,p20.
[14] Thaler, R. H., & Sunstein, C. R. (2008). Nudge: Improving Decisions about Health, Wealth, and Happiness. Yale University Press,p6.
[15] Ferguson, A. G. (2017). The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement. NYU Press,p481.
[16] European Commission. (2024). The EU Artificial Intelligence Act. Official Journal of the European Union,p50.

[17] Youmans, W. L., & York, J. C. (2012). Social media and the activist toolkit: User agreements, corporate interests, and the information infrastructure of modern social movements. Journal of Communication, 62(2), p329.

Bibliography List :

- Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, PublicAffairs, 2019, P.
- Eli Pariser, *The Filter Bubble: What the Internet Is Hiding from You*, Penguin Press, 2011, P.
- Michel Foucault, *Discipline and Punish: The Birth of the Prison*, Pantheon Books, 1977, P.
- David Lyon, *Surveillance Studies: An Overview*, Polity Press, 2007, P.
- Jeremy Bentham, *Panopticon; or, The Inspection House*, T. Payne, 1791, P.
- Cass Sunstein, *Echo Chambers: Bush v. Gore, Impeachment, and Beyond*, Princeton University Press, 2001, P.
- Richard Thaler & Cass Sunstein, *Nudge: Improving Decisions about Health, Wealth, and Happiness*, Yale University Press, 2008, P.
- Andrew Guthrie Ferguson, *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement*, NYU Press, 2017, P.
- Matthew J. Page et al., *The PRISMA 2020 statement: An updated guideline for reporting systematic reviews*, BMJ, London, Vol. 372, 2021, P.
- Katarzyna Nocun & Magdalena Pace, *Digital vigilantism: A systematic literature review*, Internet Policy Review, Berlin, Vol. 10, No. 4, 2021, P.
- Shoshana Zuboff, *Big Other: Surveillance capitalism and the prospects of an information civilization*, Journal of Information Technology, London, Vol. 30, No. 1, 2015, P.
- Mark Andrejevic, *The work of watching one another: Lateral surveillance, risk, and governance*, Surveillance & Society, Ontario, Vol. 2, No. 4, 2005, P.
- Anders Albrechtslund, *Online social networking as participatory surveillance*, First Monday, Chicago, Vol. 13, No. 3, 2008, P.
- Gilles Deleuze, *Postscript on the Societies of Control*, October, New York, Vol. 59, 1992, P.
- William L. Youmans & Jillian C. York, *Social media and the activist toolkit: User agreements, corporate interests, and the information infrastructure of modern social movements*, Journal of Communication, Oxford, Vol. 62, No. 2, 2012, P.

Additional Studies Cited:

Chen, H., et al. (2026). Attitudes Toward AI-powered Robots in Policing. Journal of Policing Studies.

Wallace, R., et al. (2026). Algorithmic tenancies and the ordinal tenant. Housing Studies.

Beissembayeva, G., et al. (2026). Algorithmic Linguistic Manipulation in Virtual Discourse. Discourse Studies.

Sot, M., & Rappas, S. (2026). Displaying devotion in social media: Letter TikToks. New Media & Society.

Moravec, P., et al. (2025). Algorithmic personalization: a study of knowledge gaps. Communication Research.

Huang, K., & Zhou, Y. (2025). Generative AI outperforms humans in social media engagement. Nature Communications.

Sombatpoonsiri, J., et al. (2026). Ramping up control: judicial harassment and online smear campaigns. Human Rights Quarterly.

Beidollahkhani, O. (2026). Regulating female embodiment as disciplining citizens. Gender & Society.