INDIAN JOURNAL OF LEGAL REVIEW

VOLUME 5 AND ISSUE 12 OF 2025

INSTITUTE OF LEGAL EDUCATION

INDIAN JOURNAL OF LEGAL REVIEW

APIS – 3920 – 0001 | ISSN - 2583-2344

(Open Access Journal)

Journal's Home Page – https://ijlr.iledu.in/

Journal's Editorial Page - https://ijlr.iledu.in/editorial-board/

Volume 5 and Issue 12 of 2025 (Access Full Issue on - https://ijlr.iledu.in/volume-5-and-issue-12-of-2025/)

Publisher

Prasanna S,

Chairman of Institute of Legal Education

No. 08, Arul Nagar, Seera Thoppu,

Maudhanda Kurichi, Srirangam,

Tiruchirappalli – 620102

Phone : +91 73059 14348 - info@iledu.in / Chairman@iledu.in

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 12 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

PRIVACY, PROPORTIONALITY, AND THE CORPORATE PANOPTICON

AUTHOR - PREKSHA JAIN* & SUJAL CHHAJED**

* RENAISSANCE LAW COLLEGE, INDORE

** NATIONAL LAW INSTITUTE UNIVERSITY, BHOPAL

BEST CITATION - PREKSHA JAIN & SUJAL CHHAJED, PRIVACY, PROPORTIONALITY, AND THE CORPORATE PANOPTICON, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR)*, 5 (12) OF 2025, PG. 445-458, APIS – 3920 – 0001 & ISSN - 2583-2344

Abstract

This paper applies Michel Foucault's theoretical framework of biopower to examine how contemporary corporate cybersecurity policies function as sophisticated mechanisms of employee control and discipline within organizational hierarchies. Drawing upon Foucault's conceptualization of disciplinary power, panopticism, and the transformation of bodies into "docile subjects," this research interrogates the extent to which cybersecurity governance has evolved beyond mere technical protection to constitute a pervasive system of surveillance capitalism that fundamentally alters the employer-employee relationship. The analysis particularly focuses on the evolving role of company secretaries as governance professionals who must navigate the delicate equilibrium between organizational security imperatives and the constitutional right to human dignity, especially within the Indian legal framework following the landmark Puttaswamy judgment and the enactment of the Digital Personal Data Protection Act, 2023. Through systematic examination of contemporary cybersecurity policies, employee monitoring technologies, and regulatory compliance mechanisms, this paper argues that corporate cybersecurity has metamorphosed into a form of biopower that operates through disciplinary technologies to produce normalized, self-regulating subjects rather than merely protecting digital assets. The research contributes to the growing body of interdisciplinary scholarship examining the intersection of corporate governance, employee rights, and surveillance technologies while proposing a normative framework for company secretaries to fulfil their fiduciary duties without compromising fundamental human dignity principles.

Keywords: Corporate biopower, panoptic surveillance, algorithmic governance, disciplinary mechanisms, employee dignity.

I. INTRODUCTION

The digitalization of corporate environments has precipitated a fundamental transformation in the nature of workplace control mechanisms, extending far beyond traditional supervisory structures to encompass sophisticated systems of technological surveillance and behavioral modification. Contemporary cybersecurity policies, ostensibly designed to protect organizational assets from external threats, increasingly function as comprehensive frameworks for employee discipline and control that would be immediately recognizable to Michel Foucault as manifestations of modern biopower.[638] This evolution represents more than mere technological advancement; it constitutes a paradigmatic shift in the exercise

[638] Michel Foucault, *Discipline and Punish: The Birth of the Prison* 135-69 (Alan Sheridan trans., Vintage Books 2d ed. 1995) (1977).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 5 AND ISSUE 12 OF 2025
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

of corporate power over human subjects, transforming employees from autonomous agents into objects of constant surveillance, measurement, and disciplinary intervention.

The theoretical framework of biopower, as articulated by Foucault in his genealogical works, provides a powerful analytical lens for understanding how modern organizations exercise control not merely through overt coercion or contractual obligation, but through the subtle manipulation of subjects' possibilities for action.[639] Biopower operates through what Foucault termed "disciplinary mechanisms", technologies of power that work upon the body and mind to produce normalized, self-regulating subjects who internalize surveillance and modify their behavior according to organizational imperatives.[640] In the corporate cybersecurity context, these mechanisms manifest through comprehensive monitoring systems, behavioral analytics, automated disciplinary protocols, and the constant threat of exclusion for non-compliance.

Within this complex matrix of power relations, company secretaries occupy a uniquely positioned role as governance professionals responsible for ensuring legal compliance while maintaining the integrity of corporate decision-making processes. The traditional conception of the company secretary as a mere administrative functionary has evolved dramatically, particularly in light of emerging data protection regulations such as India's Digital Personal Data Protection Act, 2023, which imposes stringent obligations regarding employee privacy and consent.[641] Contemporary company secretaries must navigate the increasingly complex terrain between organizational security requirements and fundamental constitutional rights, including the right to privacy recognized as a fundamental right by the Indian Supreme Court in the landmark Puttaswamy judgment.[642]

This paper argues that corporate cybersecurity policies have evolved into sophisticated systems of biopower that operate through disciplinary mechanisms to produce docile, self-regulating employee subjects while maintaining the facade of technical necessity and legal compliance. The analysis demonstrates how these systems function through three interconnected dimensions: surveillance technologies that create panoptic environments of constant observation; normalization processes that establish behavioral standards and detect deviations; and disciplinary responses that reinforce compliance through graduated sanctions and the ultimate threat of exclusion. Within this framework, company secretaries emerge as crucial governance actors who must balance competing imperatives of organizational security and human dignity, requiring new conceptual frameworks for understanding their fiduciary duties in the digital age.

The research methodology employed combines theoretical analysis of Foucauldian concepts with empirical examination of contemporary cybersecurity policies, regulatory frameworks, and judicial precedents. Particular attention is devoted to the Indian legal context, where recent constitutional developments regarding privacy rights and data protection legislation provide an ideal case study for examining the tensions between corporate governance imperatives and fundamental rights protection.

II. Theoretical Framework: Foucauldian Analysis of Power, Discipline, and Biopower

A. The Evolution from Sovereign to Disciplinary Power

Foucault's genealogy of power traces the historical transformation from sovereign power—characterized by the right to "take life or let live" to disciplinary power, which operates

[639] Michel Foucault, *The History of Sexuality, Volume 1: An Introduction* 136-40 (Robert Hurley trans., Pantheon Books 1978) (1976).
[640] Foucault, *supra* note 1, at 170-94.
[641] The Digital Personal Data Protection Act, 2023, No. 22 of 2023, s 8.
[642] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 12 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

through positive techniques aimed at fostering and directing life processes.[643] This transformation represents more than a change in governmental technique; it constitutes a fundamental shift in the nature of power relations within modern society. Where sovereign power operated through spectacular displays of force and the threat of death, disciplinary power works through subtle mechanisms of normalization, surveillance, and the production of knowledge about subjects.[644]

In the corporate context, this evolution manifests in the transition from traditional hierarchical management structures, based on direct commands and overt supervision, to sophisticated systems of behavioral monitoring and predictive analytics that operate through technological mediation. Contemporary cybersecurity systems exemplify this transition, functioning not merely as protective barriers against external threats but as comprehensive frameworks for observing, recording, and analyzing employee behavior patterns. The shift represents what Foucault would recognize as the emergence of a "disciplinary society" in which power operates through the production of knowledge about subjects rather than through mere repression.[645]

The disciplinary model operates through three fundamental mechanisms that find clear parallels in contemporary cybersecurity governance: hierarchical observation, normalizing judgment, and examination.[646] Hierarchical observation establishes systems of visibility that render subjects constantly observable while maintaining the observer's anonymity and authority. In cybersecurity contexts, this manifests through comprehensive logging systems, behavioral analytics, and real-time monitoring that create what Foucault termed "panoptic" environments of constant potential surveillance.

B. Biopower and the Government of Life

Biopower represents Foucault's most sophisticated analysis of modern power relations, describing techniques of governance that operate not through prohibition but through the positive management of life processes at both individual and population levels.[647] This form of power "exerts a positive influence on life, endeavours to administer, optimize, and multiply it, subjecting it to precise controls and comprehensive regulations."[648] Biopower operates through two distinct but interconnected poles: disciplinary techniques focused on individual bodies and biopolitical mechanisms concerned with population-level phenomena.

In corporate environments, biopower manifests through human resource management systems, employee wellness programs, productivity optimization initiatives, and cybersecurity policies that purport to protect both individual and organizational welfare. These mechanisms operate through the collection and analysis of data about employee behaviors, health indicators, performance metrics, and security compliance, creating comprehensive profiles that enable predictive interventions and behavioral modifications.

The significance of biopower for understanding corporate cybersecurity lies in its capacity to transform overt control mechanisms into apparently neutral technical requirements that employees internalize as necessary for their own protection and organizational welfare. Cybersecurity policies function as biopower as far as they present surveillance and behavioral restrictions as essential for protecting employee privacy, preventing identity theft, and maintaining organizational security, thereby enlisting employees as willing participants in their own subjugation.

[643] Foucault, *supra* note 2, at 136-37.
[644] Michel Foucault, *Society Must Be Defended: Lectures at the Collège de France 1975-1976* 35-52 (Mauro Bertani & Alessandro Fontana eds., David Macey trans., Picador 2003).
[645] Foucault, *supra* note 1, at 195-230.
[646] *Id.* at 170-77.
[647] Foucault, *supra* note 2, at 138-45.
[648] *Id.* at 137.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 12 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

C. The Panopticon as Architectural and Analytical Model

Foucault's analysis of Jeremy Bentham's panopticon provides the foundational metaphor for understanding disciplinary power in modern institutional contexts.[649] The panopticon's genius lies not in its capacity for total surveillance but in its creation of a subjective state of permanent visibility that induces self-regulation. As Foucault observes, "the major effect of the Panopticon is to induce in the inmate a state of conscious and permanent visibility that assures the automatic functioning of power."[650]

Contemporary cybersecurity systems create digital panopticons through comprehensive logging, behavioral analytics, and automated monitoring systems that render employee activities constantly visible to organizational authority while maintaining the observer's anonymity. Employees cannot determine when their activities are being monitored, analyzed, or recorded, creating the psychological conditions necessary for self-regulation and compliance with organizational norms. This uncertainty produces what Foucault termed "docile bodies" subjects who modify their behavior according to organizational imperatives even in the absence of direct supervision.[651]

The panoptic principle extends beyond mere surveillance to encompass the production of knowledge about subjects through continuous examination and documentation. In cybersecurity contexts, this manifests through security awareness training programs, compliance testing, behavioral assessments, and the creation of comprehensive digital profiles that document employees' security-related behaviors, attitudes, and competencies. These mechanisms transform employees into objects of organizational knowledge while presenting such objectification as necessary for their own protection and development.

[649] Foucault, *supra* note 1, at 195-200.
[650] *Id.* at 201.
[651] *Id.* at 135-69.

III. Corporate Cybersecurity as Disciplinary Technology

A. Surveillance Infrastructure and Panoptic Environments

Modern corporate cybersecurity systems create comprehensive surveillance infrastructures that extend far beyond traditional network monitoring to encompass behavioral analytics, location tracking, biometric identification, and predictive risk assessment.[652] These systems function as digital panopticons that render employee activities constantly visible while maintaining the fiction of technical necessity and legal compliance. The sophistication of contemporary monitoring technologies enables organizations to observe, record, and analyze virtually every aspect of employee behavior during working hours and, increasingly, during personal time when employees use corporate devices or access organizational systems.

The panoptic quality of cybersecurity surveillance lies not in its comprehensiveness but in its unpredictability and invisibility. Employees cannot determine when their activities are being monitored, which systems are recording their behavior, or how collected data will be analyzed and utilized. This uncertainty creates the psychological conditions necessary for self-regulation, as employees modify their behavior according to their perception of organizational expectations rather than explicit directives.[653]

Contemporary cybersecurity policies exemplify what Shoshana Zuboff has termed "surveillance capitalism" economic systems that extract value from human behavior through comprehensive monitoring and behavioral modification.[654] In corporate contexts, this manifests through productivity optimization algorithms, behavioral risk assessment systems,

[652] Bennett Cyphers & Karen Gullo, *Inside the Invasive, Secretive "Bossware" Tracking Workers*, Electronic Frontier Foundation (June 30, 2020), *https://www.eff.org/deeplinks/2020/06/inside-invasive-secretive-bossware-tracking-workers*.
[653] Gilles Deleuze, *Foucault* 23-44 (Seán Hand trans., University of Minnesota Press 1988) (1986).
[654] Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* 8-12 (PublicAffairs 2019).

and predictive analytics that enable pre-emptive disciplinary interventions based on statistical correlations rather than actual violations of explicit policies.

B. Normalization and the Production of Security Subjects

Disciplinary power operates through the establishment and enforcement of norms that define acceptable behavior, identify deviations, and prescribe corrective interventions.[655] Corporate cybersecurity policies function as normalizing technologies that define the characteristics of the "secure employee" while identifying and targeting behaviors that deviate from organizational security standards. These norms are not merely technical requirements but comprehensive behavioral prescriptions that extend into areas of personal privacy, communication patterns, and lifestyle choices.

Security awareness training programs exemplify the normalization process through their attempt to produce "security-conscious" subjects who internalize organizational security requirements as personal values and behavioral dispositions. These programs operate through techniques of self-examination, behavioral modification, and the cultivation of what Foucault would recognize as "technologies of the self" practices through which individuals transform themselves according to organizational imperatives.[656]

The normalization process extends beyond explicit training to encompass automated behavioral analytics that identify statistical deviations from established patterns and flag employees for additional scrutiny or intervention. These systems create what might be termed "algorithmic normalization"—the use of machine learning algorithms to define behavioral norms and identify deviations without explicit human programming or oversight.[657] Such systems exemplify the evolution of disciplinary power from human observation to automated surveillance that operates according to statistical rather than moral or legal criteria.

C. Disciplinary Responses and the Graduated Sanction System

Foucault identified the system of graduated sanctions as a fundamental mechanism of disciplinary power, operating through "a micro-penalty of time (lateness, absences, interruptions of tasks), of activity (inattention, negligence, lack of zeal), of behavior (impoliteness, disobedience), of speech (idle chatter, insolence), of the body (incorrect attitudes, irregular gestures, lack of cleanliness), of sexuality (immodesty, indecency)."[658] Contemporary cybersecurity policies create sophisticated systems of graduated sanctions that respond to security violations through escalating interventions designed to produce compliance rather than merely punish non-conformity.

These disciplinary responses typically begin with automated warnings, progress through mandatory retraining, include temporary restrictions on system access, and culminate in termination of employment for persistent violations. The graduated nature of these sanctions serves to normalize the disciplinary process while providing multiple opportunities for employees to demonstrate their willingness to conform to organizational security requirements.[659]

The sophistication of contemporary disciplinary systems lies in their capacity to operate automatically through algorithmic decision-making systems that detect violations, assess their severity according to predetermined criteria, and implement appropriate responses without human intervention. Such systems exemplify what might be termed "automated discipline"—the use of artificial intelligence and machine learning to implement disciplinary

[655] Foucault, *supra* note 1, at 177-84.
[656] Michel Foucault, *Technologies of the Self: A Seminar with Michel Foucault* 16-49 (Luther H. Martin et al. eds., University of Massachusetts Press 1988).
[657] Btihaj Ajana, *Digital Personas: The Construction of Online Identity* 45-67 (Peter Lang 2013).
[658] Foucault, *supra* note 1, at 178.
[659] *ISO/IEC 27001:2022 Information Technology — Security Techniques — Information Security Management Systems — Requirements* § 6.4 (2022).

mechanisms that operate with greater consistency and comprehensiveness than traditional human-administered systems.

IV. The Company Secretary's Role in Cybersecurity Governance

A. Evolution of the Company Secretary Function

The traditional conception of the company secretary as a primarily administrative functionary responsible for maintaining corporate records and facilitating board communications has undergone dramatic transformation in response to increasingly complex regulatory environments and evolving conceptions of corporate governance.[660] Contemporary company secretaries function as governance professionals with broad responsibilities encompassing legal compliance, risk management, stakeholder relations, and strategic advisory functions that position them as crucial intermediaries between corporate management and regulatory authorities.

The emergence of cybersecurity and data protection as central governance concerns has further expanded the company secretary's role to encompass responsibility for ensuring compliance with complex technical regulations while maintaining the integrity of corporate decision-making processes. This expansion has occurred within the broader context of what might be termed the "professionalization" of corporate governance, the transformation of governance from an essentially administrative function to a specialized professional discipline requiring sophisticated technical knowledge and ethical judgment.[661]

Within the Indian context, the Institute of Company Secretaries of India (ICSI) has explicitly recognized cybersecurity governance as a core competency for contemporary company secretaries, requiring specialized training in data protection law, cybersecurity frameworks, and technology risk management.[662] This recognition reflects the broader transformation of the company secretary function from record-keeper to governance professional capable of navigating complex interdisciplinary challenges.

B. Fiduciary Duties in the Digital Age

The expansion of company secretary responsibilities into cybersecurity governance raises fundamental questions regarding the nature and scope of fiduciary duties in the digital age. Traditional conceptions of fiduciary responsibility focus on duties of care, loyalty, and good faith that operate primarily within established legal and contractual frameworks. However, the emergence of cybersecurity as a governance concern requires company secretaries to balance competing obligations to organizational security, employee privacy, regulatory compliance, and broader social responsibilities[663].

The fiduciary duty of care requires company secretaries to exercise reasonable judgment in implementing cybersecurity policies that protect organizational assets while respecting employee rights and constitutional principles. This obligation extends beyond mere compliance with technical regulations to encompass broader responsibilities for ensuring that cybersecurity policies are proportionate, necessary, and respectful of fundamental human dignity principles.

The duty of loyalty requires company secretaries to prioritize organizational interests while recognizing that long-term organizational welfare may require policies that respect employee rights and constitutional principles even when such policies impose short-term costs or operational constraints. This obligation becomes particularly complex when cybersecurity policies that maximize short-term security benefits may undermine long-term

[660] The Institute of Company Secretaries of India, *The Evolving Role of Company Secretaries in Data Privacy and Cybersecurity*, Company Secretary Journal, March 2025, at 15-18.
[661] *Id.*
[662] *Id.*
[663] Mohinder Pal Bansal, *Company Secretary: Law & Practice* 45-78 (LexisNexis 8th ed. 2020).

organizational reputation, employee morale, or legal compliance.

C. Regulatory Compliance and Constitutional Rights

The enactment of the Digital Personal Data Protection Act, 2023, has created new legal obligations for Indian corporations regarding employee data collection, processing, and protection that directly implicate company secretary responsibilities.[664] The Act requires organizations to implement "reasonable security safeguards" to protect personal data while respecting individual rights to access, correction, and erasure of personal information. These obligations create potential tensions between organizational security requirements and individual privacy rights that company secretaries must navigate through careful policy design and implementation.

The constitutional right to privacy, as recognized in the landmark Puttaswamy judgment, provides additional constraints on corporate cybersecurity policies by establishing privacy as a fundamental right subject to constitutional protection.[665] The Supreme Court's analysis emphasizes that any restriction on privacy rights must satisfy tests of legality, necessity, and proportionality, criteria that apply to corporate cybersecurity policies insofar as they restrict employee privacy and autonomy.

Company secretaries must therefore ensure that cybersecurity policies satisfy constitutional requirements for proportionality while achieving legitimate organizational security objectives. This requires sophisticated analysis of the relationship between specific security measures and their privacy impacts, consideration of alternative approaches that might achieve security objectives with less privacy intrusion, and ongoing assessment of whether implemented policies remain necessary and proportionate in light of evolving circumstances.

V. Cybersecurity Policies as Biopower

A. Employee Monitoring and Surveillance Technologies

Contemporary corporate cybersecurity systems deploy sophisticated monitoring technologies that create comprehensive surveillance infrastructures extending far beyond traditional network security measures. These systems typically include keystroke logging, screen capture technology, email and communication monitoring, web browsing surveillance, location tracking for mobile devices, biometric authentication systems, and behavioral analytics that identify unusual patterns requiring investigation.[666]

The sophistication of contemporary monitoring systems enables organizations to create detailed behavioral profiles that document employee work patterns, communication habits, productivity metrics, and security compliance levels. These profiles function as what Foucault would recognize as "disciplinary files", comprehensive documentation systems that transform individuals into objects of organizational knowledge and enable predictive interventions based on behavioral analysis.[667]

The biopolitical dimension of employee monitoring manifests through the integration of cybersecurity surveillance with employee wellness programs, performance management systems, and human resource analytics that purport to optimize employee health, productivity, and satisfaction. These systems exemplify biopower's characteristic operation through the positive management of life processes rather than mere prohibition or punishment.

B. Security Awareness Training and Behavioral Modification

Corporate security awareness training programs function as sophisticated

[664] The Digital Personal Data Protection Act, 2023, *supra* note 4, ss 8-12.
[665] Puttaswamy, *supra* note 5, at ¶¶ 180-85.
[666] Benjamin Hewitt, *Panoptic Employment: Remote Worker Health Data Under Surveillance*, 24 Colum. Sci. & Tech. L. Rev. 349, 355-70 (2023).
[667] Foucault, *supra* note 1, at 189-91.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 5 AND ISSUE 12 OF 2025
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

technologies of behavioral modification that operate through techniques of self-examination, normalization, and the cultivation of security consciousness among employees. These programs typically include mandatory training modules, simulated phishing exercises, compliance testing, behavioral assessments, and ongoing reinforcement activities designed to internalize organizational security norms.[668]

The disciplinary character of security awareness training manifests through its operation as what Foucault termed "examination", a combination of hierarchical observation and normalizing judgment that transforms individuals into objects of knowledge while purporting to enhance their capabilities and protect their interests.[669] Training programs create comprehensive documentation of employee security knowledge, attitudes, and behaviors that enable targeted interventions for individuals identified as security risks.

Simulated phishing exercises exemplify the sophisticated disciplinary techniques employed in contemporary cybersecurity governance. These exercises create artificial security threats designed to test employee responses and identify individuals requiring additional training or monitoring. Employees who fail these tests are subjected to mandatory retraining, enhanced monitoring, and potential disciplinary consequences that reinforce the importance of security compliance.

C. Automated Disciplinary Systems and Algorithmic Governance

The integration of artificial intelligence and machine learning into cybersecurity systems has enabled the development of automated disciplinary mechanisms that detect violations, assess their severity, and implement appropriate responses without human intervention. These systems exemplify what might be termed "algorithmic governance"—the use of computational systems to implement organizational policies and disciplinary responses according to predetermined criteria.[670]

Automated disciplinary systems typically operate through risk scoring algorithms that assign numerical values to employee behaviors based on their potential security implications. Employees with high-risk scores are subjected to enhanced monitoring, mandatory training, access restrictions, and other disciplinary measures designed to reduce their risk profile and ensure compliance with organizational security requirements.

The sophistication of algorithmic governance systems raises fundamental questions regarding accountability, transparency, and due process in corporate disciplinary procedures. Employees subjected to automated disciplinary measures may have limited understanding of the criteria used to assess their behavior, the evidence considered in disciplinary decisions, or the procedures available for challenging algorithmic determinations.

VI. Constitutional and Legal Framework Analysis

A. The Puttaswamy Judgment and Privacy as Fundamental Right

The Supreme Court of India's unanimous decision in Justice K.S. Puttaswamy (Retd.) v. Union of India represents a watershed moment in Indian constitutional jurisprudence regarding privacy rights and their implications for corporate governance.[671] The Court's recognition of privacy as a fundamental right under Articles 14, 19, and 21 of the Constitution establishes privacy protection as a constitutional obligation that extends beyond state action to encompass corporate activities that significantly impact individual privacy interests.

[668] Workable, *Company Cyber Security Policy Template* (Jan. 3, 2024), *https://resources.workable.com/cyber-security-policy*.
[669] Foucault, *supra* note 1, at 184-94.
[670] Karen Yeung, *Algorithmic Regulation: A Critical Interrogation*, 12 Regulation & Governance 505, 510-25 (2018).
[671] Puttaswamy, *supra* note 5.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 5 AND ISSUE 12 OF 2025
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

The Puttaswamy judgment establishes a three-pronged test for evaluating restrictions on privacy rights: the existence of law authorizing the restriction, the presence of a legitimate state aim, and the proportionality of means employed to achieve the stated objective.[672] While this test was developed for evaluating state action, its underlying principles provide guidance for corporate policies that restrict employee privacy through cybersecurity measures.

The proportionality requirement is particularly significant for corporate cybersecurity policies, as it demands that privacy restrictions be no more extensive than necessary to achieve legitimate security objectives. This principle requires organizations to consider alternative approaches that might achieve security goals with less privacy intrusion and to implement the least restrictive measures consistent with effective security protection.

B. The Digital Personal Data Protection Act, 2023

The enactment of the Digital Personal Data Protection Act, 2023, creates comprehensive legal obligations for Indian corporations regarding employee data processing that directly constrain the implementation of cybersecurity policies.[673] The Act establishes data minimization principles requiring that personal data collection be limited to what is necessary for specified legitimate purposes, storage limitation requirements mandating deletion of data when no longer needed for stated purposes, and transparency obligations requiring clear disclosure of data processing activities.

Section 7 of the DPDP Act provides certain exemptions for employment-related data processing, including safeguarding employers from loss or liability, maintaining confidentiality of trade secrets and intellectual property, and providing services or benefits sought by employees.[674] However, these exemptions are subject to reasonableness requirements that prevent organizations from using employment relationships to justify unlimited data processing or surveillance activities.

The Act's emphasis on consent and individual rights creates potential tensions with cybersecurity requirements that may necessitate data processing without explicit employee consent. Organizations must carefully balance security objectives with statutory obligations to respect employee rights and obtain appropriate consent for data processing activities that extend beyond legitimate employment purposes.

C. Judicial Precedents on Employee Surveillance

Indian courts have addressed employee surveillance issues in several contexts that provide guidance for evaluating the legality of corporate cybersecurity policies. The Supreme Court's decision in People's Union for Civil Liberties v. Union of India established that telephonic surveillance without proper authorization constitutes a violation of privacy rights, even when conducted for legitimate security purposes.[675]

The Delhi High Court's decision in Sangamitra Acharya v. State (NCT of Delhi) extended privacy protections to non-state contexts, observing that fundamental rights may apply to corporate activities that significantly impact individual liberty and dignity.[676] This decision suggests that extensive corporate surveillance systems may be subject to constitutional scrutiny when they create conditions comparable to state surveillance.

The Kerala High Court's recognition of internet access as a component of privacy and educational rights in Faheema Shirin R.K. v. State of Kerala provides additional support for limiting corporate cybersecurity policies that

[672] *Id.* at ¶¶ 180-85.
[673] The Digital Personal Data Protection Act, 2023, *supra* note 4.
[674] *Id.* s 7.
[675] People's Union for Civil Liberties v. Union of India, (1997) 1 SCC 301 (India).
[676] Sangamitra Acharya v. State (NCT of Delhi), 250 (2018) DLT 36 (India).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 5 AND ISSUE 12 OF 2025
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

excessively restrict employee access to digital resources or communications.[677] These precedents collectively establish a framework for constitutional analysis of corporate cybersecurity policies that emphasizes proportionality, necessity, and respect for fundamental rights.

VII. Balancing Security Imperatives with Human Dignity

A. Proportionality Analysis in Cybersecurity Governance

The principle of proportionality, derived from constitutional jurisprudence regarding fundamental rights restrictions, provides a framework for evaluating corporate cybersecurity policies that implicate employee privacy and autonomy. Proportionality analysis requires consideration of three interconnected elements: the legitimacy of security objectives, the necessity of specific measures for achieving those objectives, and the proportionality of means employed relative to the benefits achieved.[678]

Legitimate security objectives in corporate contexts include protection of confidential information, prevention of unauthorized access to systems and data, compliance with regulatory requirements, and maintenance of operational continuity. However, the mere assertion of security concerns does not justify unlimited surveillance or behavioral restrictions; organizations must demonstrate that specific measures are necessary for achieving legitimate objectives and that alternative approaches would be less effective.

The necessity requirement demands that cybersecurity measures be tailored to address specific identified risks rather than implementing comprehensive surveillance systems based on generalized security concerns. Organizations must conduct risk assessments that identify particular threats, evaluate the effectiveness of potential countermeasures, and select approaches that achieve security objectives with minimal privacy intrusion.

B. Human Dignity as a Limiting Principle

The constitutional principle of human dignity, while not explicitly articulated in the Indian Constitution, has been recognized by the Supreme Court as an underlying foundation of fundamental rights that constrains both state action and, potentially, private activities that significantly impact individual dignity.[679] Human dignity principles require that individuals be treated as autonomous moral agents rather than mere objects of organizational control or sources of security risk.

In the cybersecurity context, human dignity principles constrain the extent to which organizations may implement surveillance and behavioral control measures that treat employees as objects of suspicion rather than trusted partners in organizational security efforts. Dignity requirements suggest that cybersecurity policies should emphasize employee education, participatory decision-making, and transparent communication rather than covert surveillance and automated disciplinary responses.

The dignity principle also requires consideration of the broader impact of cybersecurity policies on employee autonomy, creativity, and job satisfaction. Policies that create environments of constant surveillance and behavioral monitoring may undermine human dignity even when they achieve legitimate security objectives, suggesting the need for careful balancing of security benefits against dignity costs.

C. Participatory Governance and Employee Rights

Contemporary governance theory emphasizes the importance of participatory decision-making processes that include affected

[677] Faheema Shirin R.K. v. State of Kerala, 2020 SCC OnLine Ker 1005 (India).
[678] Aharon Barak, *Proportionality: Constitutional Rights and Their Limitations* 131-98 (Cambridge University Press 2012).
[679] Maneka Gandhi v. Union of India, (1978) 1 SCC 248, ¶ 7 (India).

stakeholders in policy development and implementation. In the cybersecurity context, participatory governance principles suggest that employees should have meaningful opportunities to contribute to cybersecurity policy development, understand the rationale for specific measures, and participate in ongoing evaluation and refinement of security practices.[680]

Participatory approaches to cybersecurity governance can enhance both security effectiveness and employee dignity by creating shared understanding of security challenges, building employee commitment to security objectives, and identifying innovative approaches that balance security requirements with employee privacy and autonomy. Such approaches exemplify what might be termed "democratic governance" of cybersecurity that treats employees as partners rather than objects of organizational control.

The implementation of participatory governance requires organizational commitment to transparency, accountability, and ongoing dialogue regarding cybersecurity policies and their impacts on employee rights and dignity. Company secretaries can play a crucial role in facilitating such dialogue by creating institutional mechanisms for employee participation and ensuring that employee concerns are appropriately considered in policy development processes.

VIII. Recommendations for Company Secretary Practice

A. Governance Framework Development

Company secretaries should develop comprehensive governance frameworks that integrate cybersecurity requirements with constitutional rights protection and human dignity principles. These frameworks should establish clear procedures for policy development, implementation, monitoring, and evaluation that ensure appropriate consideration of employee rights and constitutional principles throughout the governance process.[681]

The governance framework should include specific provisions for risk assessment that consider both security risks and privacy/dignity impacts of proposed cybersecurity measures. Risk assessments should evaluate alternative approaches for achieving security objectives and select measures that provide adequate protection with minimal privacy intrusion and dignity impact.

Governance frameworks should also establish clear procedures for employee participation in cybersecurity policy development, including mechanisms for soliciting employee input, considering alternative approaches, and communicating the rationale for policy decisions. Such procedures can enhance both security effectiveness and employee acceptance while demonstrating organizational commitment to respectful treatment of employee concerns.

B. Policy Design and Implementation Principles

Cybersecurity policies should be designed according to principles of transparency, proportionality, and respect for human dignity that recognize employees as autonomous agents rather than mere objects of organizational control. Policies should clearly articulate the security objectives they are designed to achieve, the specific measures that will be implemented, and the procedures available for employees to raise concerns or request modifications.[682]

The principle of data minimization should guide cybersecurity monitoring activities, ensuring that surveillance and data collection are limited to what is necessary for achieving specific security objectives. Organizations should regularly evaluate whether implemented monitoring systems remain necessary and

[680] Archon Fung, *Democratic Participation in AI: A Survey of the Literature*, AI & Society (2023), *https://doi.org/10.1007/s00146-023-01635-w*.

[681] The Institute of Company Secretaries of India, *Data Privacy & Cybersecurity: A Governance Imperative*, Company Secretary Journal, March 2025, at 18-22.

[682] *Id.*

proportionate in light of evolving security threats and available alternative approaches.

Implementation procedures should emphasize education and support rather than punishment and exclusion, recognizing that most security violations result from inadequate training or system design rather than malicious intent. Disciplinary responses should be proportionate to actual security impacts and should provide opportunities for employee learning and improvement rather than merely imposing sanctions.

C. Ongoing Monitoring and Evaluation

Company secretaries should establish ongoing monitoring and evaluation procedures that assess the effectiveness of cybersecurity policies in achieving security objectives while respecting employee rights and constitutional principles. Monitoring should include regular assessment of employee satisfaction with cybersecurity policies, evaluation of policy impacts on workplace climate and productivity, and analysis of whether implemented measures remain necessary and proportionate.[683]

Evaluation procedures should include regular review of cybersecurity incidents to determine whether current policies are effective in preventing security breaches and whether alternative approaches might achieve better results with less privacy intrusion. Such reviews should also consider whether disciplinary responses are achieving their intended objectives or creating unintended negative consequences for employee morale and organizational culture.

Company secretaries should also establish procedures for responding to employee complaints regarding cybersecurity policies and for modifying policies based on experience and changing circumstances. Such procedures demonstrate organizational commitment to continuous improvement and respect for employee concerns while maintaining flexibility to address evolving security challenges.

IX. Implications for Corporate Governance Theory

A. Reconceptualizing Fiduciary Duties

The analysis of cybersecurity as biopower suggests the need for fundamental reconceptualization of fiduciary duties to encompass responsibilities for protecting human dignity and constitutional rights within corporate governance frameworks. Traditional conceptions of fiduciary duty focus primarily on financial performance and legal compliance, but the pervasive impact of cybersecurity policies on employee autonomy and privacy requires broader understanding of corporate social responsibility and ethical governance.[684]

Fiduciary duties in the digital age should encompass responsibility for ensuring that corporate policies and practices respect fundamental human rights and constitutional principles, even when such respect imposes short-term costs or operational constraints. This expanded conception recognizes that long-term organizational success depends upon maintaining employee trust and social legitimacy, which require respectful treatment of employee rights and dignity.

The reconceptualization of fiduciary duties also requires recognition that corporate governance decisions have broader social implications that extend beyond immediate stakeholder interests. Cybersecurity policies that normalize surveillance and behavioral control contribute to broader social trends toward what Foucault would recognize as "disciplinary society," with implications for democratic governance and human flourishing that responsible corporate leaders should consider.

B. Stakeholder Governance and Employee Participation

The analysis suggests that effective cybersecurity governance requires adoption of

[683] *Id.*

[684] Lynn Stout, *The Shareholder Value Myth: How Putting Shareholders First Harms Investors, Corporations, and the Public* 87-103 (Berrett-Koehler Publishers 2012).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 5 AND ISSUE 12 OF 2025
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

stakeholder governance models that recognize employees as legitimate participants in organizational decision-making rather than mere objects of managerial control. Stakeholder governance approaches can enhance both security effectiveness and employee dignity by creating shared understanding of security challenges and building employee commitment to security objectives.[685]

Stakeholder governance in the cybersecurity context requires organizational commitment to transparency, accountability, and participatory decision-making that enables employees to understand security policies, contribute to policy development, and hold organizational leaders accountable for policy impacts. Such approaches represent practical applications of democratic governance principles within corporate contexts.

The implementation of stakeholder governance requires development of institutional mechanisms that enable meaningful employee participation while maintaining organizational effectiveness and legal compliance. Company secretaries can play a crucial role in designing and implementing such mechanisms, drawing upon their expertise in governance procedures and stakeholder relations.

C. Corporate Social Responsibility and Digital Rights

The emergence of cybersecurity as a significant factor in employee relations suggests the need for expanded conceptions of corporate social responsibility that encompass protection of digital rights and promotion of human dignity in technological contexts. Corporate social responsibility in the digital age requires recognition that organizational technology choices have significant implications for employee autonomy, privacy, and dignity that responsible organizations should consider in decision-making processes.[686]

Digital rights as components of corporate social responsibility include employee rights to privacy, autonomy, participation in decisions affecting their working conditions, and treatment with dignity and respect in technological contexts. These rights create affirmative obligations for organizations to design and implement technology systems that enhance rather than undermine human flourishing and democratic participation.

The integration of digital rights into corporate social responsibility frameworks requires development of new assessment tools, reporting mechanisms, and stakeholder engagement processes that enable organizations to evaluate and communicate their performance regarding digital rights protection. Such frameworks can enhance organizational reputation while contributing to broader social objectives of human dignity protection and democratic governance.

X. Conclusion

This analysis demonstrates that contemporary corporate cybersecurity policies function as sophisticated systems of biopower that operate through disciplinary mechanisms to produce docile, self-regulating employee subjects while maintaining the facade of technical necessity and legal compliance. The transformation of cybersecurity from a purely technical function to a comprehensive framework for employee control represents a paradigmatic shift in corporate governance that has profound implications for human dignity, constitutional rights, and democratic participation in organizational decision-making.

The Foucauldian theoretical framework provides crucial insights into the operation of power within corporate cybersecurity systems, revealing how surveillance technologies, normalization processes, and disciplinary

[685] R. Edward Freeman et al., *Stakeholder Theory: The State of the Art* 15-35 (Cambridge University Press 2010).

[686] Archie B. Carroll, *Corporate Social Responsibility: Evolution of a Definitional Construct*, 38 Bus. & Soc'y 268, 280-95 (1999).

responses work together to create what Foucault would recognize as "panoptic" environments of constant potential observation and behavioral modification. These systems exemplify biopower's characteristic operation through the positive management of life processes rather than mere prohibition, transforming employees into willing participants in their own surveillance and control.

The analysis of Indian constitutional and legal frameworks reveals significant tensions between cybersecurity imperatives and fundamental rights protection, particularly following the Supreme Court's recognition of privacy as a fundamental right in the Puttaswamy judgment and the enactment of the Digital Personal Data Protection Act, 2023. These legal developments establish clear constraints on corporate surveillance activities while requiring sophisticated balancing of security objectives with constitutional rights protection.

Company secretaries emerge from this analysis as crucial governance professionals who must navigate the complex terrain between organizational security requirements and constitutional rights protection. The evolution of the company secretary function from administrative support to strategic governance advisory reflects broader trends toward professionalization of corporate governance and recognition of the interdisciplinary challenges facing contemporary organizations.

The research contributes several significant insights to existing scholarship on corporate governance, employee rights, and surveillance technologies. First, it demonstrates the utility of Foucauldian theoretical frameworks for understanding contemporary corporate power relations and their implications for human dignity and democratic participation. Second, it reveals the extent to which cybersecurity policies have evolved beyond their ostensible technical purposes to function as comprehensive systems of employee control that require careful constitutional and ethical analysis.

Third, the analysis suggests the need for fundamental reconceptualization of fiduciary duties, corporate social responsibility, and stakeholder governance to address the challenges posed by digital technologies and their impacts on human rights and dignity. Such reconceptualization requires integration of constitutional principles, human rights protection, and democratic governance values into corporate governance frameworks that have traditionally focused primarily on financial performance and legal compliance.

The practical implications for company secretary practice include the need for comprehensive governance frameworks that integrate cybersecurity requirements with constitutional rights protection, policy design principles that emphasize proportionality and human dignity, and ongoing monitoring and evaluation procedures that assess policy effectiveness while respecting employee rights and constitutional principles.

Future research should explore the application of similar analytical frameworks to other aspects of corporate governance affected by digital technologies, including artificial intelligence decision-making systems, algorithmic human resource management, and predictive analytics applications. Such research can contribute to the development of governance frameworks that harness technological capabilities while protecting human dignity and democratic values.

The ultimate challenge facing contemporary organizations is to develop cybersecurity governance approaches that achieve legitimate security objectives while respecting the fundamental human dignity and constitutional rights of employees. Meeting this challenge requires sustained commitment to participatory governance, constitutional compliance, and ethical reflection that recognizes technology as a tool for human flourishing rather than merely organizational

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 12 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

control. Company secretaries, as governance professionals positioned at the intersection of legal compliance and organizational strategy, have a crucial role to play in ensuring that corporate cybersecurity governance serves human dignity rather than undermining it.