
SURVEILLANCE, STATE POWER, AND CONSTITUTIONAL SAFEGUARDS IN INDIA'S DIGITAL ERA

SECURITY
NEEDS
POWER.
DEMOCRACY
NEEDS
LIMITS.



The increasing dependence on digital technology has an impact on the use of state power, especially in relation to digital governance and surveillance. Often justified on the basis of efficiency and security, technology is increasingly being used in India for administrative purposes, national security, and law enforcement. But there are much more serious concerns about privacy, accountability, and constitutional guarantees in this increasing digital usage. The Information Technology Act of 2000 controls the application of technology in the Indian context. It evaluates whether it is consistent with the constitutional values or not. It also discusses how the Digital Personal Data Protection Act, 2023, highlighted the tension between broad state exemptions that diminish effective accountability and data protection obligations.

INTRODUCTION

In modern legal frameworks, technology has been changing the role of power over time. Modern power is often embedded in invisible digital networks, as opposed to earlier forms of power that were exercised through visible institutions such as courts and police forces. Today, computers, data collection systems, and surveillance systems are crucial to law and order. This has raised complex questions about freedom, the accountability of the state, and constitutional limits in India. While technology is often presented as a necessity for efficiency and security, the unregulated use of technology poses the danger of reducing the basic rights that the law is intended to protect.

SURVEILLANCE AND THE EXPANSION OF EXECUTIVE AUTHORITY

One of the most significant expansions of state power in the contemporary period is digital surveillance. The State is now able to monitor citizens in ways that were previously

inconceivable due to communication interception, internet activity surveillance, and data analysis. These powers are mainly employed in India through the Information Technology Act, 2000, particularly under Sections 69 and 69A, which allow information interception and blocking for purposes such as public order and national security.

Although these provisions are legal, they are mainly administered by the executive. Persons affected by these activities are hardly informed, and surveillance warrants are obtained through private means. This lack of administrative openness creates a situation where citizens are always under surveillance, but the processes of surveillance are not visible to the common man. Over time, this division has the potential to normalize excessive surveillance as a norm rather than an exception.

The absence of substantial checks on the use of surveillance powers is therefore more problematic than the existence of these powers itself. Privacy as a Constitutional Restraint.

In the case of Justice K.S. Puttaswamy vs. Union of India (2017), the Supreme Court analyzed the constitutional implications of digital surveillance and confirmed the right to privacy as a basic element under Article 21. Under this decision, any government interference that impacts the privacy of an individual must satisfy the tests of legality, necessity, and proportionality. Privacy is an essential element of liberty and dignity. This decision has created a major constitutional hurdle for surveillance practices. However, the application of these concepts is still not uniform. The assessment of proportionality is hardly ever questioned by the public or the opposing party, and the surveillance systems are still functioning with very little judicial oversight. As a result, constitutional safeguards are often more theoretical than practical in government practice.

DIGITAL PERSONAL DATA PROTECTION ACT

To deal with concerns about the misuse of personal data, the Digital Personal Data Protection Act, 2023, was proposed. The Act represents an evolution towards a broader recognition of informational rights by setting out guiding principles such as consent, purpose limitation, and data security. However, in addition to this, the Act provides broad exemptions to state authorities in relation to matters such as public order, security, and sovereignty. Such exemptions raise difficult questions about accountability. Citizens are left with little recourse in situations where the state is the primary holder of exemptions and the primary data collector. The lack of transparency in data retention and sharing policies further reduces public trust.

CONSEQUENCES OF DIGITAL MONITORING TO HUMANS

Surveillance affects people's lives, and it is more than a mere technical or legal issue. Permanent surveillance may limit political engagement and freedom of speech,

particularly among journalists, researchers, and activists. Self-censorship, which subtly challenges democratic speech, is commonly stemming from the fear of constant observation. Apart from surveillance practices, digital wrongs such as identity theft, cyberbullying, and the misuse of personal information have lasting implications for individuals. Because of procedural delays and legal intricacies, these negative consequences often resist immediate legal redress. The rapidity with which digital harm diffuses and exposes its victims to danger for protracted periods of time is in marked contrast to the delayed reaction of the law. Thus, in order to protect individual freedom in the digital age, it is necessary to recognize that harm caused on the internet has consequences that are not less than real physical pain.

SECURITY AND RIGHTS: REFRAMING THE DEBATE

Surveillance is often justified by the government as a necessary trade-off between freedom and security. This is a very deceptive way of looking at the issue. Ultimately, unaccountable security policies will damage the integrity of democracy rather than enhance public security. Overly interfering surveillance can potentially lead to a lack of trust between the citizens and the government rather than preventing threats. On the other hand, accountability enhances constitutional government and enhances the legitimacy of government action. The legal system must ensure that surveillance remains targeted, temporal, and subject to outside review.

CONCLUSION

Technology will remain a factor in the future of governance, but it is how power is exercised through technology that will shape how legitimate it is. Unchecked uses of surveillance technology have the potential to erode constitutional freedoms and make invasions of privacy the norm. Rather than resisting innovation, the role of the law is to civilize technology through institutional checks and rights. This is made possible by the Indian constitutional framework. The challenge is to incorporate constitutional values into ordinary administrative processes. It is only when the law remains vigilant against the surreptitious accumulation of unaccountable power that a technological future respects human dignity.

