NATIONAL CYBERSECURITY POLICY VS INDIVIDUAL PRIVACY IN CYBERSPACE

Alina Sadique*

ABSTRACT

Cybersecurity has become a major policy concern as states depend more and more on digital infrastructure to protect vital systems, deter cybercrime, and preserve digital sovereignty. From being a forum for unrestricted communication, cyberspace has developed into an important area for national security, economic activity, and governance. However, worries about state surveillance and the degradation of personal privacy have increased concurrently with the growth of cybersecurity measures. In order to determine whether the pursuit of digital security warrants greater state control over personal data, this paper analyses the inherent conflict between national cybersecurity policies and the right to individual privacy in cyberspace. In addition to examining the increasing dependence on surveillance technologies like data analytics and artificial intelligence, the paper charts the development of cyberspace as a matter of state interest, and keeping an eye on digital communications. It assesses critically how these mechanisms run the risk of turning cybersecurity into an instrument of excessive surveillance, even though they are intended to counter cyber threats. The study emphasises the importance of privacy in a data-driven digital economy by conceptualising it as autonomy and control over personal information rather than just secrecy. The study examines the goals and execution of national cybersecurity policies with an emphasis on the Indian context, as well as issues with accountability, oversight, and enforceability. It looks at issues like the lack of independent oversight over surveillance practices, encryption disputes, and regulatory gaps. The essay delves deeper into the moral aspects of cybersecurity governance, contending that unrestrained surveillance erodes democratic principles and public confidence. According to the study, privacy and cybersecurity are not mutually exclusive objectives. Rather, it promotes a fair, rights-abiding strategy that combines robust security

*BA LLB, FOURTH YEAR, HERITAGE LAW COLLEGE.

measures with proportionality, legal protections, and open supervision. In order to create a cyberspace where security and fundamental rights can coexist, the paper concludes that sustainable digital governance necessitates policies that safeguard both national security and individual privacy.

Keywords: Cybersecurity, Cyberspace, State Surveillance, Digital Communications, National Security.

INTRODUCTION

The virtual world is an alternate life in which people live their personal, occupational and civic lives. Cyberspace is the spirit of present-day lives, in terms of social interactions as well as in terms of money transfer. This field grows, and the issue of its security increases accordingly. Policies on cybersecurity are being developed at the national level in states around the world to mitigate cyberattacks, espionage, and misinformation on their citizens and critical infrastructure.[1] But, such a quest for safety usually clashes with the other pillar of democracy, namely, personal privacy. The conflict between the security of the Internet and the privacy of individuals characterises one of the most topical ethical and legal dilemmas of the online era.

THE EMERGENCE OF CYBERSPACE AS STATE BUSINESS

Cyberspace was initiated as a free communication and innovation sphere. It, however, became essential to the nation with the increased centrality to governance, commerce, and defence. The governments have realised that digital networks are equally important in determining the stability of the state as territorial boundaries. Cyberattacks have the potential to disrupt important services, expose defence systems, steal sensitive information and affect elections. As such, cybersecurity policy governance in the country developed to protect the integrity, confidentiality, and accessibility of information systems. These policies are usually based on the development of defensive capabilities, creation of awareness, and creation of legal frameworks aimed at preventing, detecting, and responding to cyber incidents. In India, as an example, the national cybersecurity strategy wants to develop a secure digital infrastructure, improve incident response, and improve collaboration between agencies.[2] Like blueprints, the

[1] National Cyber Security Policy 2013 (India), para 1.1.
[2] Ibid, paras 3.2-3.4.

same can be found all over the world, and this is indicative of the universality as well as the urgency of digital defence. However, with these precautions comes the threat of policing.

THE STATE SURVEILLANCE: SURVEILLANCE NECESSITY OR SURVEILLANCE OVERREACH?

State surveillance is described as the surveillance of online conduct, metadata, and digital communications by government bodies. Its advocates defend it as a necessary step to fight cybercrime, terrorism and subversion.[3] As the threats have changed to a different dimension beyond the physical boundaries, intelligence agencies say that digital spying will allow risk detection at an early stage and thus, prevent the damage before it turns into a reality.

Nevertheless, the processes that enable surveillance to work are the same processes that make surveillance intrusive. Privacy is no longer a right, especially when all digital traces of footprints, such as calls, messages, locations, searches, etc., can be traced.[4] The new surveillance technologies use artificial intelligence, data analytics, and facial recognition elements that expand the state into the realm of individual space. Such systems will be prone to slipping off course into mass surveillance without strict supervision. This is due to the asymmetry of power that has led to the dilemma.

PRIVACY IN THE DIGITIZED WORLD

Privacy is not only about secrets, but it is also about control and autonomy. It grants them the liberty to contemplate, communicate and interact without any apprehension of being observed all the time. Privacy in cyberspace means the right of an individual to control his or her personal information, which includes who gets it, how and why it is processed or used.

Privacy is an asset and a liability in the digital economy because it is data-driven. User information is regularly gathered by social media, online shopping platforms and service vendors. The boundary between legitimate investigation and intrusion is obscure when the state agencies require such data on security grounds. The ease of access to biometric identifiers, the logs of digital payment, and communication allows one to infer that the lack of protection of privacy measures once should lead to lifetime exposure due to the ease of access to such

[3] Information Technology Act, 2000, ss 69, 69A (inserted by amendment 2008).
[4] Justice K.S. Puttaswamy v Union of India (2017) 10 SCC 1, para 267 (recognising privacy as fundamental right).

records.[5] The privacy debate was prominent due to the privacy revelations of surveillance programmes around the world and domestic data breaches. People started asking themselves whether they would be safe by giving up personal freedoms. It is not about denying the possibility of surveillance but rather about making sure that the surveillance does not go beyond legal and ethical limits.

NATIONAL CYBERSECURITY POLICY: INTENTION AND PROMISE

A country-wide cybersecurity policy is the foundation of a country's digital defence strategy of a country. It establishes goals, values, and procedures to achieve cyber infrastructure security. Its major pillars tend to be:

- **Securing Critical Information Infrastructure:** Protecting the critical infrastructure of defence, energy, health and finance against cyber interference.
- **Resilience and Incident Response:** Introduction of Computer Emergency Response Teams and a system of dealing with cyberattacks.
- **Awareness and Capacity Building:** Training the government officials, entrepreneurs and citizens on safety measures.[6]
- **International Cooperation:** Communication of intelligence and resources to other countries to fight transnational cyber-attacks.
- **Lawful and Regulatory Mechanisms:** Reproduction of crimes, punishment and system of enforcement in accordance with the national law.

Ideally, a balance between national security interests and civil liberties is struck in such a policy. In reality, though, the focus usually shifts to surveillance and control, particularly at times of crisis. The problem is not the intentions of the policy but how to implement it and enforce it.[7]

ENFORCEABILITY AND SUPERVISION DEMANDS

The policies of cybersecurity in a large, dynamic digital space are complicated to implement. The pace of new technology is so fast that the regulations mostly keep up with the practice. Cybersecurity agencies are not always subject to the same jurisdiction, which may lead to

[5] Ibid, para 310.
[6] Information Technology (Critical Information Infrastructure Protection) Rules, 2021, r 3.
[7] Information Technology Act, 2000, s 70B.

regulatory conflicts. Furthermore, the control of compliance involves legal access to data, an aspect that has a direct influence on privacy. As an example, encryption technologies not only provide the safety of the communications, but also aggravate law enforcement. The idea of companies granting access backdoors to state systems has been a point of global debate in governments on whether companies should have a backdoor to lower the security standards.[8]

Another area of weakness is oversight. Without supervisory authorities, which are independent, the surveillance authority can be abused to gain political or personal interests. There must be clear standards of authorisation, proportionality, and accountability, which are to be defined by an enforceable policy. The judicial review, legislative oversight and transparency reports are pivotal to monitor state activity without interfering with national interest.

THE ETHICAL DIMENSION

Privacy and cybersecurity are not exclusive to each other, and they have a more moral relationship. Achieving true security is not possible by getting rid of the risk and thus freedom, but having a system where the two coexist. The gathering of too much information in the name of security is a state that will erode trust in the people, whereas the state that does not bother with security will bring about chaos. This is the ethical dilemma, though, of moderation, of applying surveillance as a scalpel, and not a net.

The ethical policymaking demands deference to human dignity, its proportionality in access to data, and necessity. The citizens must be educated on the principles of data processing, and the consent mechanisms should be clear and not empty. Similarly, it is the duty of state actors to realise that digital sovereignty should not be an excuse to have complete control.[9]

THE INDIAN SITUATION AND FUTURE

Cybersecurity has become a national priority in India due to the fast digital transformation in the country, which has reached e-governance up to fintech. Meanwhile, its huge number of internet users makes the issue of privacy particularly urgent. The secure digital India vision will necessitate inclusive, enforceable and rights-respecting policies. To this, some steps cannot be done without-

[8] Report of the Justice B.N. Srikrishna Committee on Data Protection (2018) 145-150.
[9] Ibid.

Enhancing the Legislation: Cybersecurity laws and data protection should be complementary and specify what the state can or cannot do.

Institutionalising Oversight: Surveillance should be audited by an independent authority, and the privacy safeguards must be complied with.

Ethics Capacity Building: Educating government and corporate staff about cyber-hygiene, privacy legislation and human-rights-centric design.[10]

Public Awareness: Citizens should know their digital rights to manage and safeguard authoritative information.

Technological Innovation: Security and privacy are both achievable via the encouragement of encryption, anonymisation, and privacy-preserving technologies.[11]

CONCLUSION

The new arena of governance is cyberspace. States should exercise restraint against the urge to go too far when formulating cybersecurity policies aimed at protecting digital sovereignty. The state does not give people any privacy, but it is a basic right that justifies its power. The security founded on suspicion will fall on its own weight; the security based on respect for rights will survive. The surveillance-privacy dilemma is fundamentally a question of values: what type of society would you like to live in during the digital era? Through accountability, transparency, and human dignity incorporated in the cybersecurity policies, countries can protect the systems and souls of their people.[12] The end is not to make a decision between security and privacy, but to create a cyberspace where both are able to co-exist.

[10] Digital Personal Data Protection Act, 2023, ss 17-18.
[11] National Cyber Security Coordinator, 'India's Cyber Security Strategy' (MeitY 2020) 12.
[12] Digital Personal Data Protection Act, 2023, ss 17-18.