Journal of Polity & Society (2025) 17(1), 189-200

State-Dominated Technological Surveillance in India: Policies of Delhi and Telangana Governments on CCTVs

RAKSHIT KWEERA
Hyderabad Central University

India is an emerging player in the study of CCTV surveillance in the Global South. The penetration of technological surveillance has increased manifold in the last decade, and this is mainly led by the state machinery in India. The government at the centre, i.e., the union government and various provincial governments within their jurisdiction, have passed laws and brought policies in this regard. The two provinces in India that stand out in terms of the use of surveillance for security are Delhi and Telangana. This is evident from the fact that Delhi and Hyderabad emerge as the most surveilled cities in the world in many reports. The police in these provinces are highly reliant on the use of CCTV cameras for security, and they have detailed laws and policies for surveillance. While charting out the laws and policies of the Telangana and Delhi governments on the use of CCTV surveillance, I will also map various stakeholders involved within the state institutions in this process, how the state dominates surveillance, and how the public has to comply with it.

Keywords: Surveillance, Security, Technology, CCTV, Facial Recognition Technology Delhi, Telangana

---

Surveillance is a phenomenon that has been around for a while. It has been there from time immemorial, but the scale, reach, and speed in present times are fascinating and troubling commentators worldwide. Informal community surveillance was used to monitor and control social activity in the premodern era, but modernity has made this role more structured and bureaucratic. Surveillance has always been an element of state power in general and an important attribute of policing in particular. If we look at the historical evidence, popular culture, and literary sources, surveillance has been identified with the state. Bentham s conception of a benign panopticon, in which we are continuously visible, is a metaphor for power to control the desired population through surveillance. We also have Foucault, who considers surveillance an important feature of the governmentality of the state, where the rationale of complete control and order is desired through surveillance. We have surveillance depicted in popular culture and fictional literary works. Orwell s novel 1984 depicts a dystopian world in which the subject population is completely controlled through the unregulated use of surveillance technologies.

That said, the state has been at the focal point of analysis in all these depictions and is the prime agent of surveillance. If we undertake a historical analysis of the state and the methods of surveillance undertaken by it, we will observe that the state has used surveillance for various purposes: The control and ordering of subjects, the

purpose of governance, and the identification of criminals/dacoits, etc. Surveillance was mainly used on the colonial subjects by the masters, but it evolved into an indispensable state mechanism. In modern nation-states, this surveillance practice has developed into a full-grown technique, and different political regimes use it directly or indirectly on their subjects.

Technological Surveillance in Theory and Practice

Surveillance as an academic research activity started in the second half of the 20th century. Although Bentham s panopticon, Foucault s panoptic gaze, and Orwellian Big Brother images had flagged issues related to state surveillance, empirically grounded studies of technological surveillance and its impact on society are only taking off now. Gary T. Marx did a detailed study of police surveillance in America. He introduced the term Surveillance Society to explain the current phenomenon of surveillance, where it seems that we are now living in a surveillance society. Marx (1998) stated that with the introduction of computer technology, one of the final barriers to total control is crumbling. Marx specifically differentiates between the old and new forms of surveillance. He says that the new surveillance may be defined as scrutiny of individuals, groups, and contexts through the use of technical means to extract or create information. He states that the central feature of the new form of surveillance is the conversion to a digital form of what is gathered (Marx, 2019, p. 20). McCahil (1998) has found that:

> One of the most significant impacts of the electronic revolution has been the remarkable capacity of the new surveillance technologies, such as CCTV, to transcend both spatial and temporal barriers. Surveillance is no longer confined to controlled and arranged spaces and no longer requires the physical co-presence of the observer. (p. 41-42)

That said, the unique feature of this new form of surveillance has been the use of technology, and governments worldwide have embraced this new form of surveillance.

Governance imperatives have always driven surveillance. State security agencies have been demanding technologies that make their tasks of security and order easier and more efficient. Security forces around the globe have been implementing surveillance technology, either physical or digital, though the scale and scope may vary. However, during the Snowden revelation of 2013, we also saw the US government s brazen use of digital surveillance in connivance with private companies. Zuboff (2019) calls this surveillance capitalism, where private companies work hand in glove with state security agencies.

In the early 2000s, some discursive events shifted the focus of surveillance to the state, and the security narrative became paramount. Lyon (2015) says that events in the early 2000s would significantly influence the course of surveillance, but it wasn t until 2010 that the possible links between them were revealed. At least in the global north, the aftermath of the September 2001 attacks (commonly known as 9/11), the London bombings of 7/7, and the Madrid train attack significantly increased security-related surveillance. In this new era of securitisation, the state s rationale for the surveillance and alignment of the public and the private sectors became justified. This affected the consensus of the world community on privacy and the dignity of life. The privacy of the individuals was traded off for security, and the state

became an unchecked force for the use of surveillance.

By looking into the citizens perspective, evidence of resentment and opposition to the state s use of surveillance and infringement of personal privacy is found. Regarding market-based surveillance, the citizens are less concerned. These differences point to Foucault s (2008) lectures on governmentality in neoliberal societies. As societies move more towards a market-oriented society, they are more bound by the rules of the market instead of the state. It seems typical to respond negatively and characterise a state actor more when they go beyond their perceived function in society. However, when market participants respond in the same way, their behaviour may be viewed as less offensive or justified. The state takes a back seat to private interests. So, in Western countries, state-based surveillance is still the most visible form of surveillance, and the security narrative is now deeply embedded in the political system. Private surveillance is secretly on the rise, but it still does not catch the public s ire. That said, in the Global South, we also witness the rise of technological surveillance where state actors emerge as the primary agents of surveillance.

Research Objectives/Questions

From the above review of the literature, it becomes evident that in most developed countries, security challenges have pushed state agencies to adopt technological measures, especially CCTVs, and institutionalise technological surveillance via different laws and policies. In India as well, the security challenges are paramount. We have external security threats such as terrorism, land encroachments, and narco-terrorism from our bordering countries, such as Pakistan and China. To deal with it, security agencies have started to deploy technologies for border surveillance and also drones for monitoring the smuggling of arms and ammunition. There are internal security threats, such as the Naxalites-Maoists insurgency, the bombing of megacities in India, and the ever-present law and order situation in urban governance.

This paper attempts to describe the laws and policies on CCTV surveillance adopted by two states in India, Delhi and Telangana. The objective is to chart out the nature of state surveillance in India via analysis of the laws and policies of Delhi and Telangana on CCTV surveillance. The rationale for the selection of these two states is that the governments in these states have specific laws on CCTV surveillance and policies that directly deal with CCTV technology in security governance. Then my research questions are as follows: How do the respective state governments in Delhi and Telangana dominate technological surveillance? What are the similarities and differences in the laws and policies of Delhi and Telangana on CCTV surveillance? How does the state remain a dominant agent in technological surveillance in India?

Research Methodology

The paper adopts a qualitative approach to study the primary research objective and answer the research questions. My method of inquiry is the comparative analysis of the laws and policy documents of the Delhi and Telangana governments on CCTV surveillance. The laws and policies were chosen based on purposive sampling, where one law of both Delhi and Telangana is analysed, and some of the policies specifically relating to the use of CCTV technology for security governance are selected for analysis. The rationale for comparing the two cases is to describe the dominant role

played by different state agents, such as police and politicians, in technological surveillance. Also, by comparing the two cases, I attempt to make some policy recommendations.

Surveillance Laws in India: Colonial to the Present Times

India was under colonial rule from the mid-18th century till it gained independence in 1947. The British colonial government was keen to control the complex, heterogeneous population and devised various surveillance mechanisms. One of them was the use of biometrics, i.e., fingerprinting, introduced in the mid-19th century. British colonialists looked to the body as the focus of scientific study to overcome their anxiety and create an efficient ordering of subjects. In other words, through visual examination of bodily characteristics, British colonialists sought to identify what they perceived to be local betrayals. Tribes were primarily identified and criminalised by fingerprinting (Waits, 2016).

The British colonial government formulated laws and institutionalised surveillance. In 1883, the Indian Telegraph Act was created to grant the government the authority to install telegraph lines on both public and private property. Thus, control over the subcontinent s telegraph infrastructure was crucial for the British. This Act is still in effect in India, and telecommunications service providers are required to maintain the utmost confidentiality in matters about authorised interception under Section 5(2) of the Indian Telegraph Act 1885, read with Rule 419 (A) of the Indian Telegraph (Amendment) Rules 2007 (Indian Telegraph Act, 2023).

After Indian Independence, successive governments passed laws and adopted policies favouring state control of surveillance. Some of them are the following: Central Monitoring System (CMS) developed by the Centre for Development of Telematics (C–DOT) that grants direct, centralised access to communications data (including mobile and landline calls, Voice over IP (VoIP) calls, emails, and Internet communication including on social media) to authorised security agencies. National Intelligence Grid (NATGRID), proposed in the aftermath of the 26/11 terrorist attack, is an initiative of the Union Home Ministry to integrate the data sources of various intelligence and law enforcement agencies to identify intelligence-related patterns. The NATGRID database collects a variety of data, such as credit card transactions, visa and immigration records, tax and bank account information, and itineraries for air and rail travel. The Centre for Artificial Intelligence and Robotics (CAIR) of the Defence Research and Development Organization (DRDO) created Network Traffic Analysis (NETRA), a program for analysing Internet traffic using preset filters. Social media sites (like Instagram, Facebook, and Twitter), emails, blogs, instant messaging, and VoIP calls (like Skype and Google Talk) are among the data kinds that NETRA is anticipated to monitor (Ramachandran, 2014).

Apart from this, the Information Technology (IT) Act of 2000 provides another feature of surveillance. The IT Act s Section 69 expands it further by allowing for the surveillance, decryption, and interception of digital data in order to look into criminal activity. Importantly, it does away with the precedent established by the Telegraph Act, which expands the scope of legal authority by requiring the occurrence of a public emergency in the benefit of public safety. Various provinces in the Indian Union, also within their jurisdiction, have opted for surveillance laws and policies with the rationale of security and public order. The specific mention is of the province of Telangana and the Union territory of Delhi, which stand out among the other

provinces of the Indian Union.

Securing the National Capital Region via CCTVs

New Delhi is the capital and a Union Territory of the Indian state. Being a Union Territory, Delhi has limited legislative powers, with the executive head being the Lieutenant Governor. Delhi also has a legislative assembly with an elected Chief Minister. The legislative powers of the assembly are confined to all the subjects, barring land, police, and public order, which is directly under the control of the President and exercised by the Lieutenant Governor. There has been a continuous tug–of–war between the two executives on the issue of power-sharing, which has been aggravated under Arvind Kejriwal, the Chief Minister of Delhi. The National Capital Territory(NCT) of Delhi is of utmost political importance to the Indian state, and the city s security agencies have broad responsibilities in this regard.

Delhi police consider surveillance an important facet of security and have been implementing various policies and programmes. Delhi police conducted an assessment of all the city s key spots as part of the *Nigheban* (Guardian/Watcher) program, creating a list of vulnerable areas that need CCTV surveillance. Individuals, Resident Welfare Associations (RWAs) and Market Welfare Associations (MWAs) were motivated to install CCTV cameras at identified spots by pooling their resources. In 2018, this scheme was carried out successfully, and the number of CCTV cameras rose to 2,23,758 (Delhi Police, 2018). Apart from the physical infrastructure of CCTVs, the Delhi police also acquired the Automatic Facial Recognition System (AFRS) in March 2018, mainly to track missing children from the city.

This software was also used during the Indian Prime Minister s Ramlila Maidan event held in December 2019 to screen the crowd. According to reports, rally attendees had to go through a metal detector gate, where a camera broadcasts their faces in real-time to a control room stationed there. The live feed was compared to the facial dataset in less than five seconds. Its purpose was to detect disruptive characters and repeat offenders. Concerns about privacy and the profiling of a certain community in this project have been brought up by activists (Mazoomdaar, 2019).

Delhi is also one of the few states that have institutionalised CCTV surveillance. Delhi Rules for Regulation of CCTV Systems in NCT of Delhi, 2018, were made in exercise of the powers conferred by sub-section (1) of Section 147 read with Section 29, subsections (b), (c), (d), (f), (l), (n), (o) and (r) of Section 60 of the Delhi Police Act, 1978 . The vision statement of the rules mentions that CCTV has become common and it plays an important role in the investigation of crime and protection of the public . It also enhances the public perception of safety. These rules apply to the installation of CCTV systems in public spaces in the NCT of Delhi. Every CCTV system owner and data controller who gathers information from a public area must notify the relevant authority (Delhi Police Deputy Commissioner of Police Licensing) of the system s location, number, and purpose, among other details, including how the data or information is used, handled, and stored. The Delhi police have become the regulating authority, and the public has to comply. The Data Controller has to ensure that the feed is not misused and shall not disclose the information to any other entity. The data collected by CCTV systems will be available on demand to the government authorities mandated by law to collect information for prevention, detection, investigation, prosecution, and punishment of offences (Home Department, 2018).

The Delhi CCTV Rules had a negative reception among the political and civil society. First, the committee formed to formulate the rules was purely an administrative committee, and elected representatives and experts were not part of it. The Aam Aadmi Party(AAP) government was critical of it at various levels. AAP government alleged that the L.G. office, with the connivance of the Home Ministry of India, was trying to regulate and take credit for the work they have been doing for the safety of the citizens by using this CCTV policy. The AAP government alleged that these rules brought license raj back to life, and the public was at the helm of licensing officers for CCTV installations. On the contrary, if we notice, the AAP government was itself pushing for the use of CCTV and surveillance and had also made poll promises to install CCTVs in the city after they returned to power in 2020.

As reported, installing 3 lakh cameras throughout the city is a massive AAP government undertaking. At least 4,000 of these cameras are to be installed in each of Delhi s 70 Assembly constituencies as part of the INR 571-crore project. Bharat Electronics Limited (BEL) was awarded the phase 1 contract to deploy 1.4 lakh cameras through November 2019. The plan calls for one RWA member, PWD officials, the Delhi Police, and a representative of the business installing and managing the cameras to have access to the camera feed. By 2020, Phase 2 will install an additional 1.4 lakh cameras. (Jeelani, 2019). This programme of the Delhi government caught the public s ire when the PWD department, in a written reply to an unstarred question in the Delhi assembly, stated that RWAs could access CCTV footage only after a go-ahead from the area MLA.

Arvind Kejriwal, Chief Minister of Delhi, had also made a poll promise to install CCTV cameras in every government school, with two cameras installed in each classroom. The project costs INR 400 crore (PTI, 2019). Apart from this, a CCTV surveillance scheme is also being run by the Delhi Transport Corporation (DTC). Dahua Technologies, a prime CCTV manufacturing company from China, has been a partner in providing CCTV services in DTC buses. Transport Minister of Delhi Kailash Gahlot had said in 2021 that All DTC and cluster buses are now fitted with 3 IP cameras, MNVR integrated with GPS device, 10 panic buttons, one display for the driver, hooter, strobe and two numbers of two-way audio communication device – one each for driver and conductor . The command and control centre (CCC) has been set up at Kashmiri Gate. In addition to CCC, each depot now has a Disaster Recovery Center, a Data Center, and a separate Viewing Center where all depot managers can see live footage (The Hindu, 2021).

So, from the above description, it is clear that Delhi is implementing technological surveillance in various sectors such as public places, semi-public places, schools, and public transport. The proliferation of CCTV surveillance in the national capital of Delhi is clear from the fact that in all sectors and agencies, including the general public, perception has shifted towards CCTV as a tool for safety and security. The modes and processes of CCTV surveillance are beginning to change. Not only have laws and policies been passed for institutionalising surveillance, but we also have CCTV security becoming a political issue where politicians make it a political pitch for promoting surveillance.

Integrating CCTVs in Security Governance in Telangana

In 2013, the province of Andhra Pradesh was bifurcated, and Telangana was

formed as a new province of the Indian Union. Hyderabad, the capital city, has always been a concern for the security agencies. The demography of the city is such that both the religious denominations, Hindus and Muslims, have almost equal proportions of the population, and the city has seen communal riots of the worst kind. The twin blasts in 2007 in the old city were a kind of watershed event in Hyderabad, after which the security, mainly the physical infrastructure, was beefed up, and the police became a crucial agent in defining the policies for security and surveillance.

In the next few years, we saw an increased CCTV camera network throughout the city. The Andhra Pradesh Public Safety (Measures) Enforcement Act 2013 & Rules was subsequently passed by the state legislature in 2013 and approved by the governor. The Andhra Pradesh government created enforcement rules to carry out the authority granted by subsection (1) of section 9 of the Andhra Pradesh Public Safety (Measures) Enforcement Act, 2013. This Act gives the state s establishments public safety measures. Even after A.P. s bifurcation into Telangana, Hyderabad remained the common capital under the Governor s supervision for not more than ten years. So, this law applies to GHMC (Greater Hyderabad Municipal Corporation) and other Telangana corporations. According to Hyderabad Police (2016), Public Safety Measures mean:

> Access Controls and Closed Circuit Television Surveillance at entry and exit points of the establishments and entry and exit points of their parking areas by installing (i) Access controls through Physical and Technical means, (ii) Surveillance through Closed Circuit Television surveillance cameras with a provision for storage of video footage for 30 days (iii) The technical equipment adhering to the specifications notified by the Government. (p. 18-19)

Modern governments have an uphill task of security where uncertainty and risks must be minimised. According to section 2(a) of the Act, for example, an establishment is any location that is frequently visited by a large number of people and has the potential to host a public gathering of 100 or more people at a time. Examples of such locations include commercial establishments, industrial establishments, places of worship, educational institutions, hospitals, sports complexes, train and bus stations, and places of organised congregations. Owners of these establishments are required to provide public safety measures to ensure the safety and security of the people who visit them.

Spaces/Contexts that are deemed to be risky are, from time to time, redefined by local governments and security agencies. In this Act, too, we see that while identifying the establishment, a Supervisory Committee consisting of a representative each from Municipal, Revenue, and Police jointly inspect the establishment duly taking into account whether there is a gathering of more than 100 people at any point of time, the threat perception of that particular establishment, the vulnerability of that particular establishment and a total number of people visiting that particular establishment in a day, etc (Hyderabad Police, 2016). If we look at this act in hindsight, we will observe that the role of the police has widened a lot. The role of police in this Act is of oversight and is regulatory. If this Act was not enough, the Telangana police launched two other initiatives for the security and surveillance of the city.

Telangana embarked on a project in 2015 that would be just the start of a phase of

new style of policing in the state. *Nenu Saitham*, which means me also , is a CCTV project started in 2015 under the guidance of the then Commissioner of Police, Hyderabad Mahendra Reddy. In this project, shop owners, complexes, etc., are encouraged to install CCTV cameras on their premises. The important part is that the police encourage them to install at least two cameras facing the street in front of their premises. The next few years saw a network of *Nenu Saitham* cameras spreading across the entire city, but even after this project, it was felt that only a few areas of the city were covered, and a large part was left behind.

So, a new project was started in 2015 called the Community CCTV Project, in which colony associations and shop associations were educated and motivated to form a community group, pool resources, and install CCTV cameras in their societies. It differs from the earlier project, where the CCTV feeds were only within their premises for a period of not longer than 30 days. Here, in the community project, the CCTV feeds are controlled at three locations. First, it is within the community hall monitored by a community association; second, a control room is established at the police station; and third, it is at the commissioner s office. In the policy document, it was stated that It is intended that an effectively installed and managed system would help in crime prevention and detection, anti-social behaviour to safeguard the safety and security of areas in general and citizens in particular (Cyberabad Police, 2015). Both the *Nenu Saitham* and Community CCTV projects put the onus on the community to invest in their safety and security, but the feeds are available to the police as well, who become the biggest beneficiaries of these projects.

Telangana police have also incorporated the use of technological surveillance in their day-to-day policing. In August 2018, Telangana police became the first police force in the country to acquire the Facial Recognition System (FRS) for mainly finding missing children and crime prevention. This technology was added to the TSCOP application, which had only previously included fingerprints. The FRS checks the image of a person through the crime and criminal tracking network system (CCTNS) and other online databases. The TSCOP mobile application, which is available to all police officers, is itself a tool of surveillance where all the traditional tasks of policing have been digitised. In one of the cases of the alleged gang rape of two sisters in Gandhi Hospital, the police used the CCTV footage from Hyderabad to Mahbubnagar and the various features of the TSCOP application to solve the case (Rathnam, 2021). The security narrative in the state is so paramount that the state, especially the police state in Telangana, is formulating policies, passing laws, launching programs, and dominating the arena of surveillance. In Telangana, the police emerge as a prominent agent of surveillance where not only are traditional tasks of policing digitised, but we also see the agents adopting different modes and processes, such as motivating and making the common citizens participate in installing CCTVs for security governance of their spaces and the city.

Comparative Analysis of Delhi and Telangana

As evident from the above analysis, both the provinces of the Indian Union, Delhi and Telangana, are highly surveilled. The respective governments of both provinces have left no stone unturned when it comes to surveillance for safety and security purposes. Security is the biggest rationale when it comes to surveillance, as Delhi is the capital, and Hyderabad has a history of communal riots. The security policies of both provinces have continuously been incorporating surveillance and proposing

to adopt various mechanisms, whether technological governance or others, to use surveillance. What makes both provinces different is that they not only formulated policies but also backed these policies by passing laws that are the command of the sovereign. The common binding element has been the Home Ministry, and the police department has become the most important stakeholder in this process.

The police department of respective provinces is the primary agent and has, in a sense, led the discourses on surveillance. However, the two states are administratively different as Delhi is a union territory, and the elected government has limited powers. In the case of Delhi, the central government and the Ministry of Home Affairs administer the police department, and the Lieutenant Governor, being the administrative head, passes the laws. So, in most cases, the elected government is not consulted, and it is generally considered that Delhi, being the capital city, needs a high level of security as all the important institutions, embassies, etc, are located in the city. Whereas in Telangana, the elected government is in charge of law-making and the police are directly under the supervision of the Home Minister, who is from the ruling party.

Surveillance is seen as a crucial element of power in security governance, and no regime wants to let go of this power because of the benefits it reaps in the short and long term. The respective provincial governments in India are continuously capturing this space, and the narrative of security and surveillance is reaping electoral benefits, too. So, when the Delhi government was curtailed of its power to deliberate on CCTV-related policies, we saw a backlash from the political leaders. The AAP party in Delhi and the Bhartiya Rashtra Samiti (BRS) party in Telangana bring in the security narrative and boost the surveillance infrastructure in the cities, which has brought safety to the citizens in general and women in particular. They go to the length of making poll promises to install CCTV cameras in public places. The background to these electoral promises, as previously mentioned, is the issue of terrorism, communal riots, and women s harassment, and CCTV surveillance is projected as a panacea for all these ills.

The qualitative difference between them is the agencies involved in surveillance. In Delhi, the police and the elected government within their respective jurisdiction are equal agents of surveillance. The AAP government brings policies for use in transport, schools, and city spaces, whereas the police bring laws to regulate the same. There is always a power tussle, and we find no clear dominating agent in this case. Both agents continuously search for spaces for dominance and, in some cases, overlap too. For instance, the AAP government CCTV program for the city involves the police as well. So, for the reasons of public perception, this tussle will continue as to who is the biggest stakeholder in security and who maintains order in the city.

In the case of Telangana, surveillance is controlled by the police administration, which is directly under the control of the ruling dispensation. Although this might be the case, we observe that the political leaders, mainly the erstwhile Chief Minister K Chandrashekhar Rao (KCR) of the BRS party, had given a free hand to the police. The BRS party considers this a win-win situation as, on the one hand, the perception of the city improves and brings a lot of investments, and on the other, it reaps electoral benefits, too, as the citizens become stakeholders in security and surveillance. The police bureaucracy is

the primary agent in Telangana as they directly control surveillance, and the laws and policies strengthen their agency in this. In Telangana, the nature of policing itself has changed, and we see that technological surveillance is embedded into the institutional structure, and the day-to-day policing tasks are digitised. The Integrated Command and Control Centre in Banjara Hills, launched in 2023, is the prime example that integrates all the policing activities in the Twin Towers. In a nutshell, Telangana is almost a police state in which surveillance is one of the most crucial elements of policing.

Policy Recommendations

In India, state agencies such as the police forces emerge as the dominant agents in technological surveillance. The integration of surveillance technologies such as CCTVs, Facial Recognition Technologies (FRT), Artificial Intelligence, Drones, etc., in policing is happening rapidly. The first recommendation is to have properly certified training modules for police personnel using these technologies in policing. The state police departments should regularly train police forces at all levels, from the constable level, to effectively use these surveillance technologies. The module also requires training on the ethical use of these technologies, as reports have suggested that CCTVs have been misused by lower-level police officers in cases of gendered crimes. The rationale for security governance and crime-free spaces will remain, and the use of surveillance technologies in policing is the need of the hour, so effective and efficient use of these technologies is necessary to avoid misuse.

Additionally, we should also have policy guidelines from the Ministry of Home Affairs on the use of surveillance technologies in policing. The public safety measures will guide the state police forces in determining the best practices and limits of using specific technologies. This will also help in bringing uniformity across the various states in India, where on the one hand, we see some states like Telangana, Karnataka, etc., using advanced surveillance technologies in policing, and on the other hand, we see some of the states relying on traditional ways of policing.

The other recommendation is to use tested and reliable surveillance technologies with inbuilt security features. The recent reports of the security vulnerability of the Chinese CCTV cameras and their impact on external and internal security are an eye-opener for security agencies, especially the police forces. The surveillance products should have a built-in privacy-by-design mechanism procured from startups and manufacturers from India after a proper security check. This is to ensure the data security of the citizens and a check on the hegemonic surveillance by the state. Additionally, it is also recommended that third-party actors regularly audit these technologies and state agencies using them. The dominance of state agencies is here to stay because of the utility of surveillance technologies in security governance. The concern, then, is to make its use ethical to ensure data privacy and the dignity of the citizens.

Conclusion

In the domain of surveillance studies, we have moved from the surveillance state to a surveillance society, the latest being surveillance culture. However, if we study Western countries and the Global South, the state still dominates the surveillance

arena. Much of that has to do with the addition of technological surveillance in security governance. In India, the state, especially the police, is commanding this arena. The province of Telangana and the Union Territory of Delhi are a live example of how the state still holds command of surveillance laws and policies. Within the state institutions, we see negotiations and sometimes power tussles to determine who the main stakeholder is in this process. In Delhi, the police under the administrative control of the central government and the democratically elected government within their jurisdiction devise laws and policies for surveillance. Meanwhile, in Telangana, the police department is under complete control in terms of policies and laws, and they are in the process of including surveillance in all policing-related activities.

References

Cyberabad Police. (2015). *Community CCTV Project Process Kit*. Cyberabad Police. https://www.cyberabadpolice.gov.in/information/cctv/5-Community-CCTV-Project-Process-Kit-Release-2.0.1-Jun-15.pdf

Delhi Police. (2018). *Delhi Police Best Practices*. Delhi Police. Retrieved from http://delhipolice.nic.in/Best_practices.pdf

Foucault, M. (2008). *The birth of biopolitics: Lectures at the Collège de France 1978-1979*. Houndmills UK: Palgrave Macmillan.

Home Department, Delhi. (2018). *Delhi Rules for Regulation of CCTV Systems in NCT of Delhi*. Delhi Home Department. Retrieved from https://home.delhi.gov.in/sites/default/files/home/circulars-orders/cctv.pdf

Hyderabad Police. (2016). *Public Safety Act*. Hyderabad Police. Retrieved from https://www.hyderabadpolice.gov.in/PDF/acts/Publicsafetyact.pdf

Indian Telegraph Act. (2023). *Indian Telegraph Act, 1885*. India Code. Retrieved from https://www.indiacode.nic.in/bitstream/123456789/13115/1/indiantelegraphact_1885.pdf

Jeelani, G. (2019, July 21). *Big Brother s watching you: AAP govt s mega project to install about 3 lakh CCTV camera*. India Today. Retrieved from https://www.indiatoday.in/mail-today/story/big-brother-s-watching-you-aap-govt-s-mega-project-to-install-about-3-lakh-cctv-cameras-1571748-2019-07-21

Lyon, D. (2015). The Snowden stakes: Challenges for understanding surveillance today. *Surveillance & Society*, *13*(2), 139-152. https://doi.org/10.24908/ss.v13i2.5363

Marx, G. T. (2019). *Windows into the soul: Surveillance and society in an age of high technology*. University of Chicago Press.

Marx, G. T. (1988). *Undercover: police surveillance in America*. University of California Press.

Mazoomdaar, J. (2019, December 28). *Delhi Police film protests, run its images through face recognition software to screen crowd*. The Indian Express. Retrieved from https://indianexpress.com/article/india/police-film-protests-run-its-images-through-face-recognition-software-to-screen-crowd-6188246/

McCahill, M. (1998). Beyond Foucault: towards a contemporary theory of surveillance. *Surveillance, closed circuit television and social control. Aldershot: Ashgate*, 41-65.

PTI. (2019, July 6). *CCTV cameras in all Delhi govt schools by November, says Arvind Kejriwal*. India Today. Retrieved from https://www.indiatoday.in/india/story/cctv-cameras-in-all-delhi-govt-schools-by-november-says-arvind-kejriwal-1563445-2019-07-06

Ramachandran, C. (2014). PUCL v. Union of India Revisited: Why India s Surveillance Law must be Redesigned for the Digital Age. *NUJS L. Rev.*, *7*, 105.

Rathnam, P. (2021, August 20). *Consensual? No rape took place at Gandhi Hospital, finds probe*. The New India Express. Retrieved from https://www.newindianexpress.com/cities/hyderabad/2021/Aug/20/consensual-no-rape-took-place-at-gandhi-hospital-finds-probe-2347200.html

The Hindu. (2021, February 25). *Minister inspects command and control centre at Kashmeri Gate*. The Hindu. Retrieved from https://www.thehindu.com/news/cities/Delhi/minister-inspects-command-and-control-centre-at-kashmere-gate/article33927697.ece

Waits, M. R. (2016). The indexical trace: a visual interpretation of the history of fingerprinting in colonial India. *Visual Culture in Britain*, *17*(1), 18-46. https://doi.org/10.1080/14714787.2016.1147978

Zuboff, Shoshana. (2019). *The age of Surveillance capitalism, the fight for a human future at the new frontier of power*. London: Profile Books.