Submission to the OHCHR—HRC62 Thematic Report on the Impact of Digital and AI-Assisted Surveillance on Assembly and Association Rights, Including Chilling Effects

Submitted by: Tech Global Institute
Date: 17 November 2025

Introduction

This submission compiles research findings on the acquisition and deployment of digital surveillance technologies in Bangladesh and India, and their impact on the rights to freedom of peaceful assembly and association. The information below is provided in direct response to the questions posed in the OHCHR's guidance note.

I. According to your knowledge/experience, how have relevant digital surveillance technologies impacted the exercise of association and assembly rights (online and offline) in your country/countries of work? Please provide details on what type of surveillance technology you are aware of being used.

A. Bangladesh

Our research at the Tech Global Institute shows sustained investment by the Government of Bangladesh in more than 160 surveillance technologies and spyware systems between 2015 and 2025, at an estimated cost of USD 184.5 million. These acquisitions include laser microphones, GSM/UMTS bugs, geolocation trackers, device identifiers, audio interceptors, network analyzers, mobile and data interception systems, voice and data surveillance suites, IMSI catchers, and both fixed and portable Wi-Fi interception tools.

Bangladesh has purchased intrusive commercial spyware from at least nine vendors, such as Pegasus (NSO Group), Predator (Intellexa/Cytrox), FinFisher, WiSpear, Verint/Cognyte, and Cellebrite. These tools enable full-device compromise, including remote activation of cameras and microphones, access to internal files, and recovery of deleted or encrypted data. In parallel, AI-enabled surveillance systems supplied by foreign firms provide facial recognition, vehicle tracking, crowd analytics, and drone-based monitoring, enabling real-time observation and identification across public spaces.

Government procurement patterns reflect a coordinated, long-term strategy to strengthen the surveillance capacities of intelligence and law-enforcement agencies. For instance, in 2018, the

cabinet reportedly approved a multimillion-dollar package of surveillance technologies for the intelligence community, meanwhile, in 2019, the National Telecommunication Monitoring Centre (NTMC) reportedly acquired a nationwide content blocking and filtering system. Between 2019 and 2021, the Executive Committee of the National Economic Council approved BDT 3.16 billion (approx. USD 25.9 million) for the Rapid Action Battalion (RAB) to procure laser listening devices, IMSI catchers, Cellebrite UFED, Wi-Fi interceptors, and drone and robot surveillance platforms. Collectively, these procurements point to a multilayered architecture encompassing interception of personal communications, device extraction, biometric surveillance, and manipulation and filtering of online information flows.

B. India

In 2021, phone numbers of 300 opposition ministers, politicians, researchers, human rights activists, and journalists in India were reported to be among the 50,000 targeted with Israeli-origin spyware Pegasus. This was met with no immediate response or investigation from the State for two months. Even when the matter was taken to the apex court, authorities failed to approach it with urgency or transparency. Though the court concluded that malware was found in 5 out of 29 phones submitted, it did not confirm it to be Pegasus, despite global evidence to the contrary. Eventually, in a hearing in April 2025, the court announced that there was “nothing wrong with having spyware” when used against “anti-nationals” and concluded that it would only examine the use of spyware if private citizens were affected. As documented by Surveillance Watch, a community-run database of surveillance technologies used across the world, communities across the South Asian region have been affected by Pegasus, including in Pakistan and Bangladesh.

Besides the use of spyware and communications surveillance, research suggests that India is becoming home to vast localised infrastructures of street surveillance, powered by ubiquitous CCTV camera networks and e-policing tools. These can be State-funded and owned, but are often operated by private entities. Facial recognition technologies, sometimes integrated with artificial intelligence, are proliferating across industries in India—especially finding use in identification and authentication for travel, attendance, and availing State schemes or welfare entitlements.

II. How do you know about it? For example, does publicly available information exist, or has there been any awareness raising or consultation with communities/civil society actors prior to the procurement and/or deployment of the technology? If any

consultations were held, how has civil society/communities' feedback been reflected in the procurement and deployment of the technology?

A. Bangladesh

Our findings draw from a yearlong investigation of public procurement records, international trade data, budget documents, and open-source and journalistic reporting, which together reveal the scale and nature of surveillance technologies acquired and deployed by the Government of Bangladesh between 2015 and 2025. Historically, there has been no consultation, transparency measures, or engagement with affected communities or civil society actors prior to the procurement or deployment of these technologies. Decisions were made within security and executive bodies without publishing impact assessments, legal justifications, or human rights safeguards. Following the publication of our research in August 2025, the interim government announced the formation of a committee to investigate surveillance equipment purchases made under the previous Awami League administration and assess their role in undermining citizens' rights.

Currently, an amendment to the surveillance provision of the *Bangladesh Telecommunication Regulation Act, 2001* is under consideration, accompanied by a brief 10-day public consultation period. The amendment proposes the establishment of the Central Lawful Interception Platform under the Ministry of Home Affairs as the legally authorised body for conducting and approving interception activities. Oversight of this platform would be entrusted to a newly created council composed of representatives nominated by the president, prime minister, and speaker, alongside retired judges. Although this structure formalizes a chain of authorization, it centralizes interception authority within the executive branch and does not create avenues for independent oversight, participatory consultation, or safeguards aligned with international human rights standards.

B. India

In India, the Right to Information law of 2005 was the primary tool to access information on surveillance technologies procured and deployed for lack of proactive transparency from State authorities. Over recent years, key provisions of the law have been immensely diluted by exempting authorities and bodies from the ambit of the act who are most likely to deploy spyware or other surveillance technologies without following due process or parliamentary procedure. This has been compounded by a data protection law that weakens accountability of public officers.

Outside of information laws, technology procurement and deployment are processes marked by executive opaqueness, and such information is not published by concerned authorities. The use of personal and meta data by local police forces in investigation and surveillance has been of wide concern in the Indian context, but due to wide exemptions offered to law enforcement agencies and intelligence bodies across most legislations in India, they are not bound to make such use public.

III. What has been the authorities' justification for the use of such technology for surveillance purposes, and on what legal grounds? Has an evidence base, or detailed justification been provided?

A. Bangladesh

Under the Awami League government, the use of intrusive surveillance technologies was justified on broad grounds such as national security, public order, and counterterrorism. However, in practice, these tools were deployed against dissenters, activists, students, journalists, and members of the political opposition, often under vague and overly broad legal provisions.

For instance, section 97A of the *Bangladesh Telecommunication Regulation Act, 2001* authorizes interception by any officer of an intelligence, national security, investigative, or law enforcement agency on ambiguous grounds and grants sweeping discretionary powers with no meaningful procedural safeguards. This statutory provision is reinforced by the constitutional framework, which protects the privacy of correspondence and communications but allows "reasonable restrictions imposed by law" in the interests of state security, public order, morality, and other broad categories.

Nevertheless, the government did not provide an evidence base, necessity assessment, or detailed rationale to demonstrate why such invasive technologies were required. Likewise, procurement and deployment decisions were not subject to reasonableness or proportionality tests, and there is no requirement for prior judicial authorization or independent oversight. As a result, interception practices expanded significantly without transparency, accountability, or compliance with international human rights standards.

B. India

In India, interception and communications surveillance is rooted in law, notably the recent Telecommunications Act of 2023 and Rules, while other forms of surveillance remain unregulated. For the most part, surveillance in India is generally underpinned by societal mistrust and inequity, and at the hands of the State, marked by executive overreach and impunity. Indian police forces use drones and CCTV cameras in a regulatory vacuum, despite being one of the largest users of them.

IV. What have been the consequences of the use of digital surveillance (targeted or mass surveillance, online or offline) on the exercise of the rights to freedom of peaceful assembly and association? Have these led to arrests, detention, prosecution, stigmatisation, denial/cancellation of protected immigration status or social benefits, or any other immediate consequences related to exercising the rights to freedom of peaceful assembly or of association?

A. Bangladesh

While there is limited publicly available information establishing a direct causal link between specific surveillance technologies and arrests, detention, prosecution, or other consequences, substantial anecdotal and contextual evidence indicates that surveillance tools and spyware systems were deployed against dissenters, activists, students, journalists, and political opposition figures. These practices operated alongside broader forms of digital repression.

Ahead of the 2018 national elections, for example, the government imposed localized internet shutdowns and temporarily blocked Skype to prevent opposition leaders from interviewing potential nominees. In 2022, mobile networks were deliberately degraded in areas where opposition rallies were held, impeding communication and assembly. Moreover, cybersecurity and online expression laws have also been routinely used to justify arbitrary arrests and detentions on vague, overly broad, or politically motivated charges. Within five years of its enactment, at least 7,000 cases were filed under the *Digital Security Act, 2018*.

These restrictions coincided with periods marked by arbitrary arrests, enforced disappearances, and extrajudicial killings, contributing to an environment in which opposition parties withdrew from national elections in both 2014 and 2023. While surveillance technologies form only one

part of this broader architecture of repression, their deployment has amplified risks for individuals exercising their rights to freedom of peaceful assembly and association.

B. India

The Indian context presents a similar picture, where it is difficult to establish causality for lack of concrete evidence and information. In 2019, local police forces used facial recognition software to profile protestors in New Delhi by matching them with facial datasets collected from pictures of the protests posted online. Union Ministers claimed in parliamentary sessions that in this incident, they "identified 1,100 people through facial recognition technology".

More recently in 2024, another state police force deployed unmanned aerial vehicles to drop tear gas shells on farmers protesting for welfare entitlements, marking the first such use of drones in India. It was not confirmed at the time if the drones possessed facial detection or recognition technologies, but it was later reported that the police force began cancelling passports and visas of farmers identified through drone and CCTV cameras to be "causing disturbances" during the protests.

About Tech Global Institute

Tech Global Institute is a digital rights nonprofit with a mission to advance equity of communities in the Global Majority on the Internet. Through evidence-based research, policy advocacy, and South-South coalition-building, we aim to strengthen design and governance accountability of technologies that have an impact on underserved communities, and amplify marginalized voices and realities in policy decision-making at a global level. More information about us can be found on our website: www.techglobalinstitute.com