Digital Surveillance and the Threat to Civil Liberties in India

Mahapatra, Sangeeta

Veröffentlichungsversion / Published Version
Arbeitspapier / working paper

Zur Verfügung gestellt in Kooperation mit / provided in cooperation with:
GIGA German Institute of Global and Area Studies

Empfohlene Zitierung / Suggested Citation:
Mahapatra, S. (2021). *Digital Surveillance and the Threat to Civil Liberties in India.* (GIGA Focus Asien, 3). Hamburg: German Institute for Global and Area Studies (GIGA) - Leibniz-Institut für Globale und Regionale Studien, Institut für Asien-Studien. https://nbn-resolving.org/urn:nbn:de:0168-ssoar-73130-3

G | G A Focus | ASIA

Sangeeta Mahapatra

Digital Surveillance and the Threat to Civil Liberties in India

GIGA Focus | Asia | Number 3 | May 2021 | ISSN 1862-359X

In India, privacy was declared a fundamental right a few years ago. Since 2013, however, the government has introduced a panoply of digital-surveillance measures, normalising the shift from targeted surveillance to mass surveillance. Attempts to integrate the public and private information of citizens without strong privacy laws and external oversight indicate India's worrying slide towards a rights-restrictive "surveillance democracy."

- The emergent surveillance regime involves the state, technological companies, and people themselves, who may collaborate to monitor fellow citizens. While those surveilled are overexposed, the surveillants remain opaque. This increases the chances of rights violations, especially of the traditionally marginalised.

- The functional scope of surveillance has increased with massive digitalisation. It is now part of governance, doubling up as an early-warning system against security threats and a behaviour-moderating system of social management and control.

- New means of surveillance include artificial intelligence (AI)-enabled facial-recognition technology and drones that have been mainstreamed into public life without statutory basis or the consent of the surveilled. Digital surveillance is cost-effective for the state, while increasing harm to the public in cases of biased databases and technological errors.

- COVID-19 has securitised the concept of public-health surveillance by conflating it with public order. This has increased the data burden on private citizens, who can be denied access to public provisions and places if they do not provide their personal information. Without proper safeguards, surveillance can become a tool of exclusion and repression.

Policy Implications

The European Union can hold India, as well as tech companies, to its own strict privacy standards. Data-driven global interactions and digital dependencies necessitate this. To prevent AI products and dual-use surveillance technologies from being used by states against their own citizens, the EU can define and list high-risk ones, deny wide exemptions to states, and incentivise privacy-focused tech. This could help signal a growing global consensus against mass surveillance.

Dr. Sangeeta Mahapatra
Visiting Fellow
sangeeta.mahapatra@giga-hamburg.de

German Institute for Global and Area Studies (GIGA)
Leibniz-Institut für Globale und Regionale Studien
Neuer Jungfernstieg 21
20354 Hamburg

www.giga-hamburg.de/en/publications/giga-focus/

Towards Surveillance Democracy

In early April 2021, as millions of Hindu pilgrims thronged the banks of the Ganges in Haridwar, India, to celebrate the festival of Kumbh Mela, artificial intelligence (AI)-enabled cameras zeroed-in on faces without masks and bodies that violated the physical-distance rule. With corona cases surging past 100,000 per day, surveillance technologies like facial-recognition cameras and drones were meant to convey a sense of security. While the pilgrims were not charged for infractions, invasive surveillance technologies and predictive policing have posed serious threats to individual liberties under the cover of community safety and crowd control.

In the past few years, police in several Indian states have routinised the use of fingerprint- and facial recognition technology (FRT) to stop and screen people on grounds of suspicion. From polling booths to public-transport systems to schools, the use of close-circuit television (CCTV) and FRT on adults and children is turning vital public spaces into privacy-violating zones. In 2019 and 2020/2021, FRT and drones were used on civilians protesting against the contentious Citizenship Amendment Act and farm laws. By scanning, recording, and storing facial and gait data of protesters, the police sought to match their images with mugshot databases (such as voter identity and driving licence) and social media pages. Such technologies tend to have high error rates and are subject to the biases of their human coders (Bailey, Burkell, and Steeves 2020). Faces can be wrongly matched, leading to false arrest. After the 2020 Delhi riots, FRT – with an accuracy rate of 2 per cent or less, as per a 2018 statement of the Delhi Police – was used to recognise over 1,900 people as rioters.

Digital surveillance enables dragnet surveillance, which makes everyone a suspect. This is ethically problematic: people are not just observed but are pinpointed and profiled without their consent.

While this indicates the policing aspect of mass surveillance, the more pervasive issue here relates to the datafication of individuals (turning the identity and activity of human beings into quantifiable data) for governance and business purposes. This exposes individuals to the constant glare of states and private companies. Martin Moore warned in *Democracy Hacked* (2018) of surveillance democracy being a distortion of digital democracy. India faces this prospect. On 16 March 2020, an investigative report revealed that the Narendra Modi government was in the final stages of creating an auto-updating "360-degree database," the Social Registry Information System, to track every aspect of the lives of every Indian (Shrivastava 2020). This would use India's Aadhaar, the world's largest biometric-identity system. There was also a proposal to geo-tag every home. As per media reports, this was to ensure welfare schemes reached their targeted groups.

Trading privacy for better governance or convenience has consequences. Regardless of the subjective prioritising of privacy by individuals, it needs to be valorised as a linchpin right. It affects the rights to speech and expression, to protest, and to not be discriminated against. Digital surveillance is more invasive than traditional surveillance. It can monitor people's activities, associations, locations, emotions, and vital signs. Privacy experts warn against reducing individuals to disembodied data; instead, citizens' data should be treated with the same

consideration as their physical well-being (van der Ploeg 2005; Radhakrishnan 2020). This is more so in the age of biometric surveillance, as any data leakage, mistake, or manipulation can lead to bodily harm in terms of denial of an individual's identity and right to access essential provisions. The COVID-19 pandemic has added to this threat by securitising public-health surveillance, making it over-reliant on tech tools.

India, therefore, represents a large digitalising democracy where, in the absence of a data-protection law, digital surveillance by multiple actors is taking diverse forms despite a Supreme Court ruling declaring privacy to be a fundamental right linked with those to life and livelihood (K.S. Puttaswamy v. Union of India 2017). This emergent surveillance regime is hence analysed here. In closing, policy recommendations are offered for the European Union on regulating surveillance technologies and ensuring data privacy for a rapidly changing environment shaped by the pandemic, with the salience of the fourth generation of human rights on digital needs having increased.

Security-Based Mass Surveillance

In 2013, before the former Central Intelligence Agency analyst Edward Snowden exposed government-sponsored mass surveillance programmes like the National Security Agency's (NSA) PRISM in the United States and TEMPORA of Government Communications Headquarters in the United Kingdom, India launched a similar surveillance behemoth: the Central Monitoring System (CMS). Like PRISM, initiated after the attacks of 11 September 2001, the CMS was conceptualised after the attacks in Mumbai of 2008 to aid counterterrorism activities. In tracking terrorist and criminal activities, it got backdoor entry to citizens' data. Strategic surveillance by democracies expanded from international to domestic communications.

The CMS signalled two key changes in old-school surveillance: First, the state announced its move from targeted surveillance of criminals to lawful interception of people's private conversations as per threat perception. Second, surveillance was no longer limited to gathering and storing data. It now involved real-time monitoring of the voice calls, Internet searches, and online activity of potentially anyone with a mobile phone, landline, and Internet connection. Unlike the NSA, which required court approval to spy on calls and emails (though without public scrutiny), the CMS could work without court or even legislative approval. Apart from no external oversight to ensure accountability and prevent the abuse of power, there is no redressal mechanism for individuals whose rights get violated.

This centralised infrastructure of surveillance has hi-tech scaffolding supporting it like the National Intelligence Grid (NATGRID), Network Traffic Analysis (NETRA), and Crime and Criminal Tracking Network Systems (CCTNS). NATGRID, conceptualised as a master database fed by several government departments and ministries, would give intelligence and investigative agencies access to citizens' data including details of bank accounts, telephone records, passports, and vehicle registration. NETRA would automatically intercept voice calls over the Internet if they were red-flagged by keywords like "bomb" and "attack." In 2014, a report based on multiple Right to Information (RTI) appeals revealed

that more than 100,000 telephone interception orders were issued by the central government each year (SFLC 2014). This figure could be much higher if orders by various state governments were tallied. The CCTNS is an online tracking system for crimes and criminals linking 14,000 police stations.

This infrastructure has grown. India is set to create the world's largest government-operated facial-recognition database, the Automated Facial Recognition System (AFRS) – with an estimated budget of INR 308 crore (USD 41.62 million; EUR 34.58 million). This would identify anyone from CCTV and video by matching facial biometrics with images from multiple sources. As police often use vague terms like nabbing "suspicious individuals," "habitual protesters," and "rowdy elements" to justify their use of FRT (Bhandari 2021), this could be used to criminalise protest and curb dissent. While civilians first came under security-based surveillance, they were further exposed by governance-based surveillance.

Governance-Based Mass Surveillance

Surveillance as part of governance was brought to the forefront by Aadhaar ("Foundation" in Hindi), as launched in 2009. It provides Indians with a 12-digit unique identity number based on their biometric and demographic data to facilitate access to public goods and services. It received legal backing in 2016, but raised serious privacy concerns when the government started pushing people to link their Aadhaar ID with phone numbers, bank accounts, pensions, and similar – exposing them to the state's disciplinary gaze. This was done by aggregating confidential information about individuals to create their digital duplicate. This made it difficult for people to carry out everyday transactions without having this digital duplicate. For example, a national-election survey conducted by the Delhi-based research organisation CSDS-Lokniti in 2019 showed that due to the linking of ration cards with Aadhaar, a number of respondents from low-income groups were denied food grains either because they did not have an Aadhaar ID or due to technical glitches (Sardesai 2021). Aadhaar was transforming an essential norm of people providing their private information based on "informed consent" to that of now "compelled consent."

In 2018, during Supreme Court hearings, a group of lawyers warned against linking Aadhaar with the National Register of Citizens (to document legal citizens). The Modi government plans to implement this across India. The lawyers feared this could be used for "blacklisting" individuals as non-citizens, denying them access to welfare provisions (Bhatia 2020). Now there is a proposal for a National Digital Health ID, which would store an individual's health-related information. In the absence of a data-privacy law, the state could be privy to the most intimate details of a citizen if this is eventually linked with Aadhaar (Chandran 2020). This could especially affect sexual minorities. Further, this data could be used for other purposes as this policy allows the state to share anonymised data with third parties. If this health ID is made mandatory, it would mean a denial of certain related services to those who decide to opt out.

Apart from harm by the state, people are vulnerable to external parties in case of data breaches too. In May 2017, for example, India's Centre for Internet and Society pointed out that 130 Aadhaar numbers along with other sensitive

data were available on the Internet. Digital surveillance, while expanding the powers of states to surveil, has also brought on board private actors with even greater capacities to grab mass data. Social media platforms emerged as data-rich sites of surveillance.

Social Media Surveillance

Canadian political-communications expert Vincent Mosco (2014: 10) spoke of a surveillance state reinforced by "surveillance capitalism" (companies using big-data analytics to track and target users for profit). In the EU, the scale of this tracking is reduced due to the General Data Protection Regulation 2016/69 (GDPR). In India, tech platforms can easily surveil users. India has not enacted its Data (Privacy and Protection) Bill 2017 and Personal Data and Information Privacy Code Bill 2019 (modelled after the GDPR). The latter, in its current form, gives wide exemptions to the government in accessing people's sensitive personal data.

Freedom House's "Freedom on the Net 2019" reported that governments are increasingly relying on social media to spy on their citizens. In 2019, Facebook in its "Transparency Report" stated that India was second only to the US in requesting the company provide users' data; it had complied in 53 per cent of cases. In 2020, two years after the Supreme Court stopped the government from creating a Social Media Communication Hub to monitor the social media accounts of citizens, the Modi administration started planning for a surveillance tool to monitor individual users. Forty government departments already have access to a social media surveillance tool called Advanced Application for Social Media Analytics (AASMA) to collect live data of users from multiple social networks, do sentiment analysis on the content they post, track their location, and alert authorities accordingly.

With social media, surveillance functions and laws evolved – from the interception of voice calls by the Indian Telegraph Act (1887) to interception of digital communications by the Information Technology Act/IT Act (2000, 2008) to monitoring online media content by the IT (Intermediary Guidelines and Digital Media Ethics Code) Rules (2021). The state could legally monitor digital content on any device or platform and prosecute anyone for vaguely stated offences like threats to the sovereignty, integrity, or security of India or having friendly relations with foreign states. Arresting people for satire or criticism of the government is a new form of repression. Several states in India have misused the IT Act to arrest people for social media posts (Section 66A of the Act) and to block/takedown web pages and accounts (Section 69A of the Act). The fact that social media was now a space of surveillance had a chilling effect on self-expression. The Supreme Court repealed Section 66A in 2015, but the police still use it to make unconstitutional arrests regardless.

Social media surveillance adopts the tactic of "content moderation." On 12 February 2021, during the farmers' protests, Twitter blocked 97 per cent of the accounts the Modi government ordered it to. These accounts had been highly critical of the government. The online space, projected as the stronghold of free speech, was further gagged by the IT Rules passed on 25 February 2021. The

government could now decide which social media posts, streaming shows, and digital news could be taken down. Even the final frontier of privacy – encrypted services like WhatsApp – has come under the state's scrutiny. In the past five years, WhatsApp claims to have securely delivered over 100 trillion messages to over two billion users globally, with India being its largest market. The government could ask companies to break their own privacy-respecting encryption.

Industry Support

Private companies are equipping the state with new means of surveillance. The "Spy Files" project of the whistle-blower website Wikileaks revealed Indian companies to be in the top league of the global surveillance industry. With law enforcement and military agencies as their major clients, Indian companies have been innovating on facial- and fingerprint recognition, predictive intel, decryptors, and, now, COVID-19 tech for homeland security.

Companies like FaceTagr and StaqU provide FRT and AI solutions to police. Mobineer Info Systems is building a smart-policing app called E-Beat Book for foot-patrol police that would include FRT to match people's faces with databases and obtain information on them rapidly. Kommlabs Dezign sells interception solutions that reveal what people sound and feel like, and not just what they say. They have AI-enabled solutions to detect cognitive and emotional stress in voice calls. Like FRT, Emotion Recognition Technology is the sunrise sector of the surveillance industry. It is highly controversial, as biases are baked into the system. This can lead to a future where someone is arrested because they sound guilty. India is also among the leading countries in CCTV surveillance. Videonetics helps in video surveillance. Shoghi Communications provides surveillance tech to national-security agencies. ClearTrail and Comtrail provide tech for the interception and monitoring of voice and internet data. Foreign companies like, among others, China's ZTE, Japan's NEC, the US's Verint Systems, and Germany's FinFisher and Utimaco add to this arsenal.

Lateral Surveillance

The state's power to surveil people for security and governance, boosted by tech and private companies, has another supportive actor: people themselves. In February 2021, the Ministry of Home Affairs launched a controversial programme inviting private citizens to report on unlawful activities on the Internet and social media. The Indian Cyber Crime Coordination Centre (14C) invited citizens to become Cyber Volunteer Unlawful Content Flaggers, Cyber Awareness Promoters, and Cyber Experts. The fear is that citizens who support the ruling party can easily volunteer as Content Flaggers to muzzle critics and dissenters and get them arrested, similar to China's community monitors under its grid-management system of granular surveillance. This fear is real: a database on sedition cases compiled by Article 14, an Indian news and investigations site, revealed that 96 per cent of those filed against 405 individuals for criticising politicians and governments over the last decade were registered after the Modi government came to

power in 2014 (Purohit 2021). Human Rights Watch in its "World Report 2020" also documented the growing arrest of critics and opponents of ruling political parties both at the centre and in some states. These cases were often filed by partisan supporters.

Another variation of this surveillance has been vicious trolling as well as threat of arrests for online content the public supporters of the ruling party describe as being anti-Indian or hurting religious sentiments (Ellis-Petersen 2020). Societal distrust grows as people censor one another. Citizens are no longer community-level watchers and reporters. Instead, they are arrogating to themselves policing powers (Swaminathan and Saluja 2021).

Pandemic Surveillance

The pandemic has encouraged citizen vigilantism powered by the rationale of public health. In 2020, there were cases of Residents Welfare Associations (self-administering bodies in housing complexes and colonies) in the northern cities of Noida and Gurugram forcing residents, visitors, domestic workers, and other service providers to use the government's contact-tracing app Aarogya Setu ("Bridge of Health" in Hindi). They acted as extensions of the state. The government would make the app mandatory for travel to public or private workplaces and by train, subway, and airplane.

This represents a new normal of surveillance: people were now asked to wear or carry the means of their own surveillance. This body-tagged (wearable devices) and geo-tagged (smart device-based pandemic trackers) surveillance is not limited to identifying and isolating infected individuals, but fining and arresting them in case of lockdown or quarantine violations. There are currently 120 contact-tracing apps across 71 countries in existence. As per the COVID-19 Digital Rights Tracker, Aarogya Setu is the most downloaded among them (with more than 100 million users). It has privacy issues, as it is seeded with people's personal details. It uses static identifier (reducing potential for anonymity), and collects more information than required – thus violating the "purpose limitation" (data collected for a specific purpose and not used for other ones), "data minimisation" (basic amount of data collected to fulfil a specific purpose), legality, and proportionality requirements of India's privacy ruling of 2017 and the GDPR (Internet Freedom Foundation 2021). On 30 March 2021, an RTI document by lawyer Saurav Das revealed that the Jammu and Kashmir administration had shared the app's data about people's health with the police, violating purpose limitation.

Sensitive health data needs the highest level of protection. Aarogya Setu, however, does not hold the government liable for violations of data privacy. It also demonstrates the pitfalls of techno-solutionism, as it is not error-proof. There have been incidences of false negatives and false positives. India, like 21 other countries including Australia, France, and the US, is using drones to surveil people and enforce COVID-19 measures. Drones capture body and location data, and are not bound by privacy clauses. This has generated deep-seated fear among the surveilled, increasing the stigmatisation and targeting of already-vulnerable groups like women, Muslims, daily wage earners, gig workers, and the transgender community (Radhakrishnan 2020).

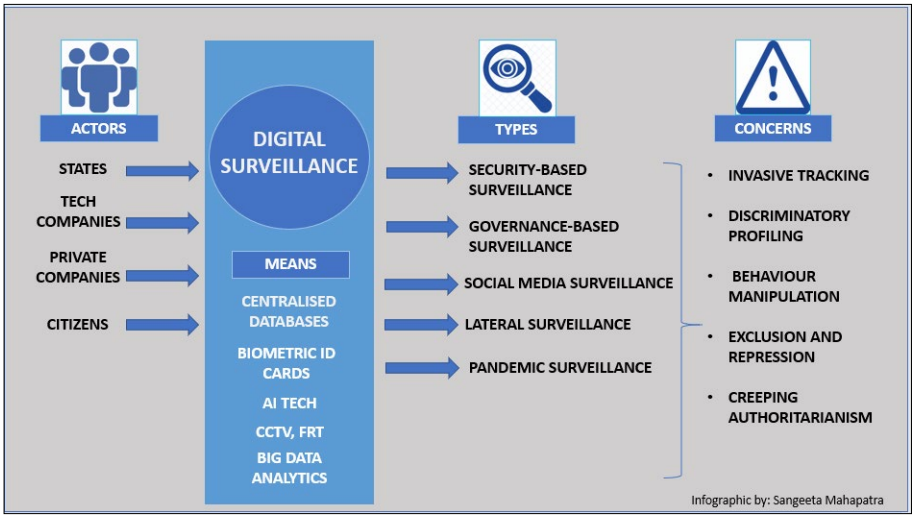

Figure 1
Digital Surveillance Matrix
Source: Author's own compilation.

In a continuation of the government's practice of digitally interlinking databases, Aarogya Setu has been integrated with the vaccination portal Co-Win. The Internet Freedom Foundation has warned this may lead to passive surveillance of those who register and denial of services to those who do not. Also, the National Health Authority of India is planning to make access to vaccines contingent on identity verification through FRT, an imprecise technology. This could lead to "potentially life-threatening exclusion" (@internetfreedom 19 April 2021).

A few states in India have come up with their own contact-tracing apps: for example, Karnataka's Quarantine Watch requiring sharing of selfies as part of quarantine verification and Jharkhand's Sahayta ("Help" in Hindi) requiring migrants to register with selfies, bank details, and Aadhaar number to receive financial support. In case of technical problems, they could be denied such assistance.

Pandemic surveillance also involves social media surveillance. On 25 April 2021, for example, as the country battled with more than 300,000 COVID-19 cases per day and acute shortages of oxygen, intensive-care-unit beds, and critical medicines, the Indian government asked Facebook, Twitter, and Instagram to take down around 100 posts and accounts panning their handling of the pandemic. Twitter geo-blocked 52 tweets, including one of a member of parliament and one of a member of the legislative assembly.

Public health should be about medical solutions, not surveillance that criminalises people. COVID-19 provides the inflection point for a transvaluation of surveillance. Urgent policies are needed for course-correction.

Safeguards Against Surveillance

Multi-actor and diverse means of digital surveillance require multilevel responses. The EU can strengthen their standard-setting role here. The Indian case offers comparative lessons, as the EU member states are themselves increasingly deploying FRT and biometrics for mass surveillance (Nash 2021). There is a need to heed the authoritarian creep in democracies enabled by digital surveillance. Also, the fact that data-driven global exchanges need mutual privacy protection has raised the stakes. The EU may hold countries like India with whom they closely engage to strict privacy- and human rights standards.

For India, legal guidelines have already been laid down by the 2017 Supreme Court ruling and "Justice A.P. Shah Report" (2012) on privacy. These are in line with Articles 12 and 17 of the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, the United Nations General Assembly Resolution on the Right to Privacy in the Digital Age (A/Res/68/167), and the GDPR.

To prevent big-data misappropriation through security- and governance-based surveillance, the EU may nudge states like India to adopt a privacy law that does not give wide exemptions to the government. This law may extend the definition of unfair trade practices to include harmful types of data surveillance. This law could discourage practices like centralised databases that integrate public and private information or compel people to barter biometric data for public goods. Privacy experts in India have suggested having separate databases with purpose and storage limitations. They also recommend a rights-respecting pandemic surveillance that does not reveal the personal details of people in contact-tracing apps and criminalise the afflicted.

Beyond India, certain global measures are needed to prevent tech-enabled abuse. Surveillance tech developed and exported by the EU countries has been used by states against their own citizens. Two recent EU measures seek to counter this. While laudatory, they need work. The first is the EU's rules on dual-use surveillance tech adopted in March 2021. Now reasons for approving or denying export licences would be made public, and surveillance tech would have to pass the human rights test. To ensure compliance, the EU may need to expand the definition of "cyber surveillance" to include biometric forms, update the list of cyber-surveillance applications that pose a high risk to civil liberties, and make state and corporate actors clearly liable for violations. The second is the EU's framework to regulate AI practices that cause physical and psychological harm, as published in April 2021. This proposal falls short of fully proscribing discriminatory AI applications by giving exemptions to the state. Advocacy groups like European Digital Rights have asked the EU to draw clear red lines against harmful AI and ban risky tech like FRT.

Apart from the human rights aspect, the EU can enhance the economic value of privacy. GDPR drove the establishment of many privacy-related tech start-ups around the world. In India, as in Europe, there is a growing demand for privacy-by-design products, browsers, and messaging services. Economic policies by the EU that incentivise privacy- rather than surveillance tech may compel big and emergent tech companies to value privacy as part of their business model. This could work alongside strengthening Internet-governance norms to debar trackers from profiling people, algorithms from manipulating them, and states from coercing platforms into giving them sensitive user data and censoring people in the name of content moderation.

This emergent surveillance regime, as exemplified by the case of India, necessitates an expanded definition of "the right to privacy." People should have a say in the rules governing their own surveillance. The current pandemic has made this of the essence, as control over data is control over bodies.

References

Bailey, Jane, Jacquelyn Burkell, and Valerie Steeves (2020), *AI Technologies, Like Police Facial Recognition, Discriminate Against People of Colour*, www.gizmodo.com.au/2020/08/ai-technologies-like-police-facial-recognition-discriminate-against-people-of-colour/ (17 February 2021).

Bhandari, Vrinda (2021), Facial Recognition: Why We Should Worry the Use of Big Tech for Law Enforcement, in: Kritika Bhardwaj, Sangh Rakshita and Shrutanjaya Bhardwaj (eds), *The Future of Democracy in the Shadow of Big and Emerging Tech*, New Delhi: National Law University Delhi Press, 97–112.

Bhatia, Gautam (2020), India's Growing Surveillance State, in: *Foreign Affairs*, www.foreignaffairs.com/articles/india/2020-02-19/indias-growing-surveillance-state (21 February 2020).

Chandran, Rina (2020), *Privacy Concerns as India Pushes Digital Health Plan, ID*, 22 September, www.reuters.com/article/india-health-tech-idUKL8N2G536U (19 February 2021).

Ellis-Petersen, Hannah (2020), *Online Hate Campaign Target Indian Streaming Stars*, www.theguardian.com/world/2020/jul/03/online-hate-campaign-targets-indian-streaming-stars (28 February 2021).

Internet Freedom Foundation (2021), *Hindsight is 20/20: Assessing Outcomes from Aarogya Setu*, https://internetfreedom.in/the-past-and-future-of-aarogya-setu/ (25 April 2021).

Mosco, Vincent (2014), *To the Cloud: Big Data in a Turbulent World*, New York: Routledge.

Nash, Jim (2021), *Privacy Advocates Push for Strict Biometric Surveillance Regulation in Appeals to White House, EU*, www.biometricupdate.com/202102/privacy-advocates-push-for-strict-biometric-surveillance-regulation-in-appeals-to-white-house-eu (18 February 2021).

Purohit, Kunal (2021), *Our New Database Reveals Rise In Sedition Cases In The Modi Era*, www.article-14.com/post/our-new-database-reveals-rise-in-sedition-cases-in-the-modi-era (2 February 2021).

Radhakrishnan, Radhika (2020), *"I Took Allah's Name and Stepped Out": Bodies, Data and Embodied Experiences of Surveillance and Control During COVID-19 in India*, https://datagovernance.org/files/research/1606371784.pdf (12 January 2021).

Sardesai, Shreyas (2021), *When Aadhaar-Related Problems Lead to Denial of Rations and Benefits: What the Data Show*, https://indianexpress.com/article/explained/explained-when-aadhaar-related-problems-lead-to-denial-of-rations-and-benefits-what-the-data-show-7277092/ (18 April 2021).

SFLC (2014), *India's Surveillance State*, https://sflc.in/sites/default/files/wp-content/uploads/2014/09/SFLC-FINAL-SURVEILLANCE-REPORT.pdf (27 January 2021).

Shrivastava, Kumar Sambhav (2020), *Documents Show Modi Government Building 360 Degree Database To Track Every Indian*, www.huffpost.com/archive/in/entry/aadhaar-national-social-registry-database-modi_in_5e6f4d3cc5b6dda30fcd3462 (15 September 2020).

Swaminathan, Mira, and Shubhika Saluja (2021), *Widening the Horizons of Surveillance: Lateral Surveillance Mechanisms: Issues and Challenges*, https://cis-

india.org/horizonsofsurveillance (17 January 2021).
Van der Ploeg, Irma (2005), Biometrics and the Body as Information: Normative Issues in the Socio-Technical Coding of the Body, in: David Lyon (ed.), *Surveillance as Social Sorting: Privacy, Risk, and Automated Discrimination*, New York: Routledge, 57–73.

About the Author

Dr. Sangeeta Mahapatra is a Visiting Fellow at the German Institute for Global and Area Studies (GIGA). She was previously a Fulbright Research Fellow at the Mershon Center for International Security Studies, Ohio State University, US, and Executive Editor of *Business Economics* magazine, India. Her research areas include digital political communications and participation, digital surveillance and privacy, and disinformation and online radicalisation.
sangeeta.mahapatra@giga-hamburg.de,
www.giga-hamburg.de/en/team/18978976-mahapatra-sangeeta/

Related GIGA Research

Dr. Sangeeta Mahapatra is a member of the GIGA's Research Programme 1 on "Accountability and Participation," which looks at processes of democratic erosion or reversal that have affected new and established democracies across continents. Within this framework, she is working on a Mozilla-funded project on "Digital Surveillance and Understanding its Chilling Effect on Journalists: Finding Strategies and Solutions to Safely Share and Seek Information Online." The research question addressed is on the protection of vulnerable citizens in a culture of civic surveillance in democracies; in this case, professional journalists reporting on marginalised communities. Focusing on India, the world's largest democracy, she examines the impact of digital surveillance on the freedom of the press and of speech and expression.

Related GIGA Publications

Grauvogel, Julia, and Christian von Soest (2021), *Cyber Sanctions: Increasing Application of a New Instrument*, GIGA Focus Global, 3, April, www.giga-hamburg.de/en/publications/24454778-cyber-sanctions-increasing-application-of-a-new-instrument/.
Mahapatra, Sangeeta, and Johannes Plagemann (2019), *Polarisation and Politicisation: The Social Media Strategies of Indian Political Parties*, GIGA Focus Asia, 3, March, www.giga-hamburg.de/en/publications/11575625-polarisation-politicisation-social-media-strategies-indian-political-parties/.
Plagemann, Johannes, Sandra Destradi, and Amrita Narlikar (eds) (2020), *India Rising: A Multilayered Analysis of Ideas, Interests, and Institutions*, The Oxford International Relations in South Asia Series, Oxford: Oxford University Press.

Sombatpoonsiri, Janjira (2021), *From Repression to Revolt: Thailand's 2020 Protests and the Regional Implications*, GIGA Focus Asia, 1, February, www.giga-hamburg.de/en/publications/23883153-from-repression-to-revolt-thailand-2020-protests-and-regional-implications/.

Sombatpoonsiri, Janjira (2018), *Manipulating Civic Space: Cyber Trolling in Thailand and the Philippines*, GIGA Focus Asia, 3, June, www.giga-hamburg.de/en/publications/11574071-manipulating-civic-space-cyber-trolling-thailand-philippines/.

Imprint

The German Institute for Global and Area Studies (GIGA) publishes the Focus series on Africa, Asia, Latin America, the Middle East, and global issues. The GIGA Focus is edited and published by the GIGA. The views and opinions expressed are solely those of the authors and do not necessarily reflect those of the institute. Authors alone are responsible for the content of their articles. GIGA and the authors cannot be held liable for any errors and omissions, or for any consequences arising from the use of the information provided.

The GIGA is thankful for the institutional support provided by the Free and Hanseatic City of Hamburg (Ministry of Science, Research, Equalities and Districts) and the Federal Republic of Germany (Federal Foreign Office).

General Editor GIGA Focus Series: Prof. Dr. Sabine Kurtenbach
Editor GIGA Focus Asia: Prof. Dr. Heike Holbig
Editorial Department: Dr. James Powell, Petra Brandt

GIGA | Neuer Jungfernstieg 21
20354 Hamburg
www.giga-hamburg.de/en/publications/giga-focus/
giga-focus@giga-hamburg.de

GIGA
German Institute for Global and Area Studies
Leibniz-Institut für Globale und Regionale Studien