Civil liberty in the Age of Digitalisation (Privacy)

– Vrinda Bhandari*

Introduction

We are living in an age of digitalisation, where growth in technology and big data has made it possible to collect, store, process, share and use personal information to create a rich profile of a person—a feat unimaginable, even a decade ago. This has created a public policy conundrum over balancing the benefits of big data with threats to the right to privacy. In an environment of pervasive surveillance and intrusive technology, available both to the State and private sector, there is a need for improved *legislative* protection of privacy rights.

Key Areas of Concern

1. *Weak regulation and oversight of surveillance activities*

India has traditionally had weak regulation of surveillance and oversight of law enforcement agencies, with four main problems:

- Lack of statutory basis for various law enforcement and intelligence agencies ["**LEAs**"] that often conduct the surveillance, such as CBI,[1] Intelligence Bureau ["**IB**"], and R&AW.
- Lack of judicial oversight over the decision to place an individual under surveillance compounded by no parliamentary accountability over the functioning of these LEAs. These problems are exacerbated by limited state capacity.
- Illegally obtained evidence is admissible under law,[2] thus distorting incentive structures.
- Telecom licenses are used to slip in surveillance provisions.

---

* Vrinda Bhandari is an Advocate practicing in the Supreme Court of India.

[1] In **Navendra Kumar v. Union of India**, W.A. No. 119/08, the Division Bench of the Gauhati High Court on 06.11.2013 held that Resolution No. 4/31/61-T dated 01.04.1963 issued by Secretary to the Government of India constituting the CBI is ultra vires; that the CBI is neither an organ nor part of the Delhi Special Police Establishment Act; and that it cannot be treated as a police force constituted under the Act. The High Court's reasoning was based on the fact that no "police force" could be empowered to investigate crimes if it had been constituted by a mere resolution of the MHA in the purported exercise of its executive powers. It further held that the impugned resolution was not 'law' within the meaning of Article 13(3)(a) of the Constitution, and the executive instructions therein could not be regarded as "procedure established by law" under Article 21. However, the Supreme Court on 10.11.2013 stayed the operation of the High Court's judgment, and there has been no movement on the matter ever since.

[2] *Pooran Mal v. Director of Inspection (Investigation),* (1974) 1 SCC 345; *State v. Navjot Sandhu,* (2005) 11 SCC 600.

2. *The absence of a data protection law*

Despite many attempts,[3] India still does not have a data protection/privacy law. Our current legal framework comprises primarily of the Telegraph Act and the Information Technology Act ["**IT Act**"], which regulate telephone tapping and electronic surveillance respectively.

Apart from this, the IT (Reasonable security practices and procedures and sensitive personal data or information) Rules 2011 provide limited protection to users against private entities.

However, this regime is inadequate and ill-equipped to deal with the privacy-incursions caused by rapidly changing technologies and business models of technology giants such as Google, Facebook, Amazon. In fact, both in the nine-judge bench privacy judgment ["***Puttaswamy* (Privacy)**"] [4] and the Aadhaar case ["***Puttaswamy* (Aadhaar)**"],[5] the Supreme Court highlighted the need for a strong data protection framework and requested the government to act expeditiously on the recommendations of the Justice Srikrishna Report.

3. *Proposed amendments to other laws*

Various Bills were passed in the Winter Session of the Lok Sabha in 2018, including:

- Aadhaar and Other Laws (Amendment) Bill – which re-introduces private sector involvement through proposed amendments to the Telegraph Act and the Prevention of Money Laundering Act and the insertion of section 4(4) permitting an "entity" to perform authentication if it is compliant with (future) privacy standards "as may be specified by regulations". It also re-introduces section 33(2) authorising the disclosure of identity information and authentication records on the decision of the Secretary.

- DNA Technology (Use and Application) Regulation Bill, 2018 – which envisages the creation of National and regional DNA Databanks, both for criminal and civil disputes, without providing adequate safeguards on the collection, storage or use of such sensitive data.

Apart from this, MHA issued a notification on 20.12.2018 authorizing 10 LEAs to conduct electronic surveillance under Section 69 of the IT Act and MEITy invited comments on the Draft Intermediary Guidelines 2018.

[3] Privacy Bill, 2011; Personal (Data Protection) Bill 2014; Data and Privacy Protection Bill, 2017.
[4] *K.S. Puttaswamy v Union of India*, (2017) 10 SCC 1 ("Privacy").
[5] *K.S. Puttaswamy (II) v Union of India*, (2018) 12 SCALE 1 ("Aadhaar")

The combined effect of these measures is to increase the surveillance powers of the State and promote proactive censorship by internet service providers, resulting in a chilling effect on the exercise of free speech.

Proposed Solutions

1. *Surveillance reform*

The Supreme Court is currently seized[6] of matters challenging the constitutional validity of various surveillance provisions, including section 69 of the IT Act, the accompanying Rules, and the MHA Notification dated 20.12.2018. The challenge is predicated on the standards of necessity and proportionality that have been recognized by the Court in *Puttaswamy* (Privacy) and *Puttaswamy* (Aadhaar).

It is recommended that the government undertake comprehensive surveillance reforms – either through the data protection law (by incorporating a new Chapter on surveillance in Justice Srikrishna's Draft Personal Data Protection Bill, 2018 [**"Draft Bill"]**) or through separate legislation – before the Court gives a final decision.

The following provisions should be in incorporated in the present legal regime, (i) to better balance privacy and security concerns, (ii) to reduce the chilling effect caused by the fear and threat of surveillance, and (iii) to stave of a potential adverse judicial ruling:

- *Prior judicial review*: Under the Telegraph Act and the IT Act, only the Executive decides whether to place an individual under surveillance. In response to an RTI, the government stated that in 2013, on average 7500-9000 orders for interception of telephones and 300-500 orders for interception of emails were being issued by the Central Government monthly.[7] The figures at the State level would thus, be even greater.

  Under the Aadhaar (Amendment) Act passed by the Lok Sabha, the Secretary who can authorise the disclosure of sensitive information or authentication records in the "interest of national security". Even the Draft Bill of 2018 grants an exemption from following data protection obligations, if the processing of data is in the "interests of security of the State".

  The common thread running through these provisions is the absence of judicial oversight in invoking the national security exception. For instance,

[6] Notice was issued by the Supreme Court in *Internet Freedom Foundation v Union of India*, W.P. (C) No. 44/2019 on 14.01.2019.
[7] Response given by the Home Ministry to the Lok Sabha on 25.05.2011; SFLC.in, "*Surveillance – Is there a need for judicial oversight*", 25 September 2013, < https://sflc.in/surveillance-there-need-judicial-oversight>.

under the IT Act, the direction to monitor/intercept/decrypt a person's information is given by the competent authority or one of the 10 LEAs. There is no judicial oversight over this decision to place an individual or "class of persons" under surveillance, either at the *ex ante* and *ex post/*review stage.

Interestingly, according to the Srikrishna Committee, the lack of legislative/statutory inter-branch oversight in India was "*not just a gap that is deleterious in practice but, post the judgment of the Supreme Court in Puttaswamy, potentially unconstitutional*". After taking into account the experience of other countries such as U.K., USA, South Africa, the Committee concluded that executive review alone is not in tandem with comparative models in democratic nations. Even the Supreme Court in *Puttaswamy* (Aadhaar) seems to have struck down section 33(2) of the Aadhaar Act for the lack of judicial review.

The Telegraph Act and IT Act also provide for a "Review Committee", comprising only of (three) members of the Executive, to review the directions/orders for surveillance. As noted in the Srikrishna Committee Report, the Review Committee usually convenes once every two months, and has the "unrealistic task" of reviewing more than 15,000-18,000 surveillance orders in every meeting. It is thus clear that no proper application of mind can take place on every interception order, to determine if it is lawful or not.

Thus, it is imperative that Parliament amends the law to provide for judicial oversight in any case where civil liberties are being impacted in the name of national security or public emergency.

- *Accountability mechanisms*: The standards of necessity, proportionality and due process laid down by the Supreme Court in *Puttaswamy* (Privacy) require an element of transparency and accountability in the functioning of LEAs. This can be achieved through parliamentary or independent oversight, which would require the Central and State Governments and the LEAs to provide an overall account of their functioning (e.g. number of requests, type of surveillance carried out, average duration of surveillance, reasons for the same etc.) and their budgetary outlays.

- *Incorporating data protection & privacy principles into current laws*:

    - Necessity, i.e. determining whether there is a less onerous means of achieving a particular government objective (such as preventing incitement of a cognizable offence) *and* whether there is an alternative way of acquiring the information.

- Collection Limitation, i.e. only such amounts of data are intercepted, monitored, or decrypted, or such calls are tapped, as are necessary/required for the limited, specific purpose of the competent authority.

- Purpose Limitation, i.e. data that is collected, monitored, intercepted, decrypted by one of the notified agencies/Central/State Government should not be disclosed to any other body without a judicial warrant.

- *Provision of the right to challenge and seek appropriate redress against unauthorised surveillance activities*.

    - Every individual should have the right to challenge and seek appropriate redress against surveillance activities. This requires that the individual be informed, as far as possible, about being placed under surveillance *after* the completion of surveillance operations.

    - The right to redress would also require amending the existing provisions of the Telegraph Act, IT Act, and the Code of Criminal Procedure to stipulate that illegally obtained communication or documents, such as through unlawful surveillance, shall be inadmissible in evidence.

    - A separate right to redress should be provided to intermediaries to question the scope and purpose of the orders received by them from LEAs under Section 69(3) of the IT Act.

- *Removing surveillance provisions in telecom licenses*: Telecom licences should not contain additional requirements, beyond the existing statutory framework, that requires telecom and internet service providers to facilitate lawful interception or conduct decryption. Current government surveillance programs such as the Central Monitoring System (**CMS)** are incorporated within the telecom licenses, without having a statutory basis in law.[8] This is clearly unconstitutional and needs to change.

2. *LEA Reform*

[8] Amendment to Condition 41.16 of the UASL, 11 October 2013, available at <http://dot.gov.in/sites/default/files/DOC231013-005.pdf?download=1>; Amendment to Condition No. 8.2 of Part II of the Unified License Agreement, 11 October 2013, available at <http://dot.gov.in/sites/default/files/DOC231013.pdf?download=1>; and Amendment to the Cellular Mobile Telephony Services (CMTS) License Agreement, 11 October 2013, available at <http://dot.gov.in/sites/default/files/DOC231013-006.pdf?download=1>.

The Intelligence Services (Powers and Regulation) Bill, 2011 was introduced as Private Member Bill in the Lok Sabha in 2011, to regulate the manner of functioning and exercise of powers of LEAs, specifically IB, R&AW, and the National Technical Research Organisation (functioning under the control of the Prime Minister).

The Bill provided for a Designated Authority for authorisation procedures and systems of warrants (for surveillance), and established a National Intelligence Tribunal for investigating complaints against these three agencies. It sought to achieve effective oversight through the creation of a National Intelligence and Security Oversight Committee, while also providing for an Intelligence Ombudsman for efficient functioning of the agencies.

However, the Bill lapsed, leaving many LEAs such as IB, R&W, and CBI vulnerable to a legal and constitutional challenge. Thus, the government should enact a similar law to provide a statutory basis for all LEAs and to regulate their functioning.

3. *A new data protection law*

The government urgently needs to enact a comprehensive data protection law, especially given the amendments proposed to other laws and the increasing influence of the private sector over our lives. Despite the Srikrishna Committee submitting a Draft Bill to MEITy, no further developments have been reported.

Hence, this section will make a few significant recommendations to Justice Srikrishna's Draft Bill:

- **Definitions**
    - **Section 3(20)** "genetic data" only covers coding DNA, and excludes non-coding DNA, even though they may be used to for DNA profiling or establishing a person's identity, genealogy, or kinship.

    - **Section 3(21)** "harm" should include harms that may arise in the future/ due to technological innovations such as loss of confidentiality of personal data, or the manipulation and change of behaviour caused by a combination of big data analytics and behavioural economics.

    - **Section 3(35)** on the definition of "sensitive personal data" should be amended to provide for contextual classification, to allow for flexibility where certain categories of personal data can become sensitive personal data, such as communication surveillance data.

- **Non consensual** processing of personal and sensitive personal data is permitted under **Sections 13 and 19** if it is "necessary for any function of Parliament or State Legislature" or for the exercise of the functions of the

State for "the provision of any service or benefit to the data principal from the State".

- Making the provision of personal data as the *basis* for enjoying certain (undefined) benefits ignores the rights of citizens to enjoy these benefits and the duty of the welfare State to provide for them. Even if these sections have to be kept, the standards need to be clearly defined, and should curtail government discretion in making a final determination on this issue.

- The terms "service" or "benefit" have to be defined, especially after the contest over their definitions in the Aadhaar debate.

- There is no requirement to follow the judicially-mandated standards of proportionality in these cases, which should be made explicit.

- The term "strictly necessary" has to be given some meaning while permitting non-consensual processing for sensitive personal data.

- **On transparency and accountability**
  - **Section 32** on data breach notifications has to be completely redrafted to provide an independent duty to inform the individual in *all* instances that their data has been breached.

  - The Bill should require the Data Protection Authority ["**DPA**"] to ensure transparency in the discharge of its functions and engage in public consultation before notifying (important) regulations

- **Section 41** on **data localization** or cross border transfer has to be changed/removed since it is overly broad, has limited benefits, and imposes huge costs, including an increased risk of surveillance.

- **Exemptions**

  - **Sections 42** and **43** exempts LEAs from most of the obligations under the Bill in the interests of the "security of the State" or "prevention, detection, investigation and prosecution of any offence…." respectively. They have to be amended, since they do not state who has to make such determination, nor do they provide for any judicial review of the decision to invoke these sections.

  - Further, **Section 43** should introduce an obligation to follow the procedure set out under the authorising law, as stated in section 42.

- **The DPA** should include part-time expert members, and the process of the selection of its members should be more detailed. Most importantly, the regulatory and adjudicatory function should not both be housed within the DPA, and the appointment of the Adjudicating Officers should not be completely at the behest of the Central Government.

4. *Adequate pre-legislative consultation*

The release of the White Paper and the Final Report by the Srikrishna Committee and Draft Bill were both followed by public consultation, which will hopefully reflect in the final text of the Bill approved by Cabinet. However, no such/adequate pre-legislative consultation was followed preceding the introduction of the Aadhaar Amendment Act or the DNA Bill, nor have they been referred to the Parliamentary Select Committee.

Given the wide ranging privacy impact of these Bills, it is recommended that all such Bills engage in a wide-ranging public consultation, and that the concerned Ministry make the responses public.

Reading Materials

- *K.S. Puttaswamy v Union of India*, (2017) 10 SCC 1 ("Privacy").
- *K.S. Puttaswamy (II) v Union of India*, (2018) 12 SCALE 1 ("Aadhaar")
- Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, "*A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians*" (2018), <http://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf>
- Personal Data Protection Bill, 2018, <http://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill%2C2018_0.pdf>
- Rishabh Bailey, Vrinda Bhandari, Smriti Parsheera, Faiza Rahman, "*Comments on the (Draft) Personal Data Protection Bill*, 2018", < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3269735>
- India Privacy Code, 2018, < https://saveourprivacy.in/bill>.
- Rishabh Bailey, Vrinda Bhandari, Smriti Parsheera, Faiza Rahman, "*Use of personal data by intelligence and law enforcement agencies*", NIPFP (2018), <http://macrofinance.nipfp.org.in/PDF/BBPR2018-Use-of-personal-data.pdf>
- Suhrith Parthasarthy, "*Towards a Genetic Panopticon*", The Hindu, 21 December 2018, <https://www.thehindu.com/opinion/lead/towards-a-genetic-panopticon/article25791126.ece>