theirview

The curious case of FIR by the UIDAI

Apart from a financial audit, the Aadhaar Act fails to prescribe any ex-ante or ex-post accountability mechanisms

VRINDA BHANDARI AND RENUKA SANE
are, respectively, a practising advocate and an associate professor at the National Institute of Public Finance and Policy.

RAMESH PATHANIA/MINT

Recently, the Unique Identification Authority of India (UIDAI) filed a first information report (FIR) against a reporter of *The Tribune* for unauthorized access of Aadhaar data (for a story that exposed the vulnerability of the Aadhaar database), and for allegedly violating the provisions of the Aadhaar Act. Last year, the UIDAI filed an FIR against a CNN-News18 journalist for a report on how it was possible to obtain two separate Aadhaar enrolment numbers. In contrast, the UIDAI did not initiate criminal prosecution against any of the 210 government websites that displayed the details of Aadhaar number holder, nor did it file an FIR against Airtel, when it was found out that Airtel used the Aadhaar-eKYC-based verification process to open payments bank accounts of its subscribers without their consent. These instances are interesting for two reasons.

First, it seems that over the last seven years since Aadhaar has been operational, we have heard of only the UIDAI filing FIRs. Second, it seems that some cases are pursued, while others are not. Why might this be?

The answer lies in Section 47 of the Aadhaar Act. This section only permits the UIDAI to initiate criminal prosecution for any violations of the Aadhaar Act, while eliminating the involvement of the Aadhaar number holder entirely. Suppose you were a victim of fraud by an enrolment agency or your personal data had been stolen from the centralized Aadhaar database. What are the choices you have? Unfortunately, under the current framework of the Aadhaar Act, you have only one choice. Let the UIDAI know, and hope that the UIDAI files a case on your behalf.

Such a provision is unique, since Indian law rarely, if ever, empowers a third party to file a criminal complaint on behalf of an aggrieved individual, to the exclusion of that individual. It is almost as if when there is a theft in your house, the best you can do is to tell your local residents welfare association, and hope that they file a case on your behalf. Parliament had obviously intended that, notwithstanding the provisions of the Indian Penal Code, certain actions should be specifically penalized under the Aadhaar Act.

Nevertheless, having designated certain actions as criminal offences, the Act deprives aggrieved individuals from accessing the criminal justice system.

Some may argue that there is a good reason for giving all the power to the UIDAI—despite the inherent conflict of interest in the UIDAI being responsible for ensuring the confidentiality of identity information of individuals, while also having the sole prerogative to initiate criminal prosecution in case of a security breach or violation of the Act. Perhaps as an administrative and regulatory body, it has the wherewithal to deal with our broken criminal justice system that we as individuals will find hard to navigate. But this is pure speculation, since we have no explanation from the drafters of the law, nor any parliamentary debates, to help explain why such a contrarian position was taken.

If the law takes away the power from you to file a complaint, and gives it to a third party, namely the UIDAI, you might expect that it imposes concomitant obligations on the UIDAI *qua* you. After all, the UIDAI is meant to be acting on your behalf. Unsurprisingly, perhaps, this is not the case. There is nothing in the Aadhaar Act, or the accompanying regulations that require the UIDAI to give details about the number of FIRs filed by it annually, or to explain why it chose to drop one complaint, or pursue another. Nor does the Act provide the aggrieved individual with any remedy if the UIDAI decides that their complaint is not worth pursuing. In contrast, even the Code of Criminal Procedure (CrPC) provides judicial recourse to an individual if the police fails to register an FIR.

Notably, as revealed by Right to Information (RTI) queries, between September 2010 (when the first Aadhaar number was issued) and October 2016, the UIDAI received 1,390 complaints about enrolment agencies, but registered FIRs in only three cases, with the other cases being "resolved", "dropped", or "closed". In fact, the UIDAI has only filed 30 FIRs till date.

This is only one of the many serious flaws in the existing Aadhaar legal framework, but it is illustrative of the weak accountability mechanism embedded in the Aadhaar Act for the UIDAI (for more on this, see *https://goo.gl/ysGQGg*).

The UIDAI is responsible for the enrolment and authentication process, data quality, security and confidentiality of data, and grievance redress. However, apart from a financial audit, the Aadhaar Act fails to prescribe any ex-ante or ex-post accountability mechanisms. In fact, the Aadhaar Act does not even require the UIDAI to inform the Aadhaar number holder if their data has been compromised.

Some have argued that a data protection authority (DPA) will solve these problems. A data protection framework and a DPA will certainly be a step forward in addressing some of these concerns, but no such law exists yet. In any event, a DPA will be burdened with far more than Aadhaar, and it seems strange to wait for the setting up of a new agency, instead of fixing the problems in the agency designed specifically to deal with Aadhaar.

Till then, we will be left with a situation where an agency that is holding our data in public trust and is supposed to work in our best interest, is choosing to go after those individuals who are exposing the vulnerabilities in the Aadhaar framework, rather than those responsible for exploiting the vulnerabilities. Unfortunately, there is nothing that we can do about it.

Comments are welcome at theirview@livemint.com