The Biometric Identification of 1.3 Billion Indians. Interview with Christophe Jaffrelot and Nicolas Belorgey

Christophe Jaffrelot, Nicolas Belorgey

The Biometric Identification of 1.3 Billion Indians.
Interview with Christophe Jaffrelot[1] and Nicolas Belorgey[2].

1 - Sciences Po, Center for International Studies (CERI), CNRS, Paris, France
2 - CSH, Centre de sciences humaines de New Delhi, CNRS

In 2009, India embarked on a scheme for the biometric identification of its people. The idea behind the project was to use digital technology—and the data collection it enables—for economic ends. But to register the entire Indian population, the state had to be persuaded to be involved in the project, later named "Aadhaar". What have been the implications of this programme, in terms of privacy in particular? How has the population reacted and are the data protected? Interview with Christophe Jaffrelot and Nicolas Belorgey, authors of the 251st Etude du CERI entitled, *L'identification biométrique de 1,3 milliard d'Indiens. Milieux d'affaires, Etat et société civile* ("Biometric Identification of 1.3 Billion Indians. The Business Community, the State and the Civil Society," November 2020).

India launched a programme for the biometric identification of its population in 2009. Who supported the project in the country and what challenges did it aim to meet?

The programme that was set up in 2009 is quite original in that the initiative came from Nandan Nilekani—one of the founders of one of the leading Indian IT companies, Infosys. But even if the high-tech business community is at the core of the project, its implementation was only possible from the moment Nilekani convinced the state of its interest and the Unique ID Authority of India (UIDAI) was created. Nilekani soon became the UIDAI's first president and R.S. Sharma, a senior state official, its first chairman. The institution was a strange body: on the one hand it was linked in an organic way to the government (Nilekani had the same status as a minister and had a privileged access to Prime Minister Manmohan Singh's cabinet, sometimes to Singh himself) and to the administration (as showed by Sharma's position); on the other hand, the UIDAI was truly autonomous, something Nilekani had negotiated fiercely and that he used fully. This is how the UIDAI subcontracted the data processing to many private companies.

The two actors—the business community and IT engineers on the one hand and the government on the other—had two distinct objectives. The first was to make a maximum of profit with the private data collected (with reference to *data being the new oil*) and with the use of digital tools in general (to simplify and secure all sorts of financial operations). The second and third objectives were the state's, which sought to reduce expenditures and corruption during social transfer operations (help to the poor, food allowances) and, later, to give each resident of India—a country where many people had no ID document—an ID number. It would not be an exaggeration to say that the first actor used the second to receive authorisation and the necessary help to successfully complete the Aadhaar (literally, the "foundation") project without the state having clearly realised the aims the business community was pursuing.

How has the programme been set up in a country as vast and rural as India, and how has the population reacted to the collecting of their private data?

The challenge was huge because it was not easy at all to collect the fingerprints and iris scans from more than a billion people in a territory as vast as the European Union with uneven transport infrastructures and frequent power cuts. For those who have written the official history of the Aadhaar programme, this feat is the result of the project architects'

motivation, the means they had at their disposal, and the sense of *jugaad* (resourcefulness) of the project engineers and operators. But this story needs to be tempered because one of the reasons why this "achievement" was possible is that the Indian population was eager to have its data collected and processed, although this desire was sometimes ambivalent. On the one hand, for many, possessing an Aadhaar number was reassuring. It meant that their identity was acknowledged, that they existed in the eyes of the state; this number was a sign of recognition. But on the other hand, part of the population had no choice but to register because it was the only way to continue to receive social allowances (the poor) or pensions (the retired), and to pay taxes. To all these legal obligations were added other, illicit, ones, notably with some banks requiring to know the Aadhaar number of their clients, or even associating it to their cell phone number.

Was there any political or institutional (judicial or legal) opposition to the project?

Aadhaar was quickly opposed by NGOs who claimed that the programme would cause many problems for the poor. In our study, we show that Aadhaar was based on a technological utopia because the project could only succeed if the digital (and electrical) network worked—which it rarely does in the depths of the Indian countryside. In addition, this technological dystopia prevented anyone whose fingerprints were erased, or whose iris was damaged because of cataracts—or who could not go or travel to have their data collected—from accessing their social allowances or pensions (a problem that did not exist before because social and family allowances were not given to individuals but to families).

The opposition expressed by NGOs defending the rights of the poor have not received much attention and the protest only became audible in the public arena when members of the middle class felt trapped and forced to register on Aadhaar to pay their taxes, for example. This is when the case was brought before the court. But the judicial battle came to a sudden end: first, the Supreme Court was so far from considering the issue a priority that when it eventually rendered a decision the judges were faced with a *fait accompli* because the collection of all the data was done, or almost. Second, the Court approved the creation of this huge database but reaffirmed that, contrary to the government's allegations, the respect of private life was a fundamental right of the citizens. The Court therefore forbid some provisions of the law that allowed the communication of the data to banks and telephone operators. But the government circumvented this decision by amending by ordinance two laws—the Prevention of Money Laundering Act and the Telegraph Act—in order to make the sharing of the data possible. The Supreme Court has not been a sufficient shield, and neither has the Parliament. In fact, MPs managed to pass the Aadhaar Bill as a *money bill,* a financial law for which adoption by the governing party does not need the upper chamber's approval (where it did not have the majority). Of course, the opposition went to court arguing that the bill had much more than financial provisions, but the Supreme Court found nothing to object to... not surprising at a moment when judges tend to avoid any confrontation with the executive power.

What about the security of the data collected?

It seems that the national biometric database has not yet been hacked. It is stored in a central server for the entire country, something that makes the entire apparatus both well-guarded and very fragile. The dataset is highly secured but the stakes are so high that according to some specialists, their theft is just a question of time. And the World Economic

Forum even declared that the risks of cyber-attacks and theft of data are among the highest globally for years to come.

Meanwhile, partial data leaks have been noticed on multiple occasions, sometimes jeopardizing people's privacy. People's identities may have been stolen, whether their numbers, used in the form of fake cards sold for a few rupees, or their fingerprints, reproduced by gangs in wax... or even by banks that stored them on reading terminals similar to smartphones. The massive recourse to private intermediaries to operate the identification chain, from initial registration to authentication operations, did not contribute to securing the whole process. In addition, the connection between the unique identifier and other information in more or less public databases has made it possible for anyone to cross-reference personal information. At some point, thousands of datasets containing an identifier as well as the name, phone number, religion, and a whole series of characteristics for a person were available online, for free.

Has the programme kept its promises? What does it bring to the population? and to the Indian state?

Mostly, the programme has enabled the large firms of the digital economy to considerably increase their turnover by decreasing their client acquisition costs and their transaction costs. In only four years the telephone company Jio has become the leader in the field, thanks also to a fierce price battle against the holders of the market. From the point of view of business, the Unique ID (UID) appears to be a way of outsourcing to the state the identification of clients with all of the costs and risks this entails—we are thinking here of companies' legal responsibility in the event of personal data theft introduced by the European Union through the GDPR. For the time being, the increase in turnouts has not (yet) generated massive profits but it does represent a long-term investment in the collection and processing of personal data. The recent financial backing by some of the so-called Gafam to the very indebted Jio confirms this analysis.

As for the Indian state, or rather, the Indian states, they have found two main benefits through the programme. First, they have increased their surveillance capacity, as illustrated by the development of the biometric clocking of civil servants, in a country where their absenteeism is deplored by many people. Second, the cleaning of public databases has allowed budgetary savings. But this final argument which was widely used as a justification for the launch of Aadhaar in the 2010s needs to be reconsidered because this "cleaning" in fact often meant... the suppression of many beneficiaries' social rights, in many cases to their utter despair.

The result of this programme is indeed a problem for the population. Certainly many people benefited from receiving smartphones with enough memory and large storage capacity for a reduced price in exchange for sharing their personal data. Some members of the middle classes have also appreciated an increased efficiency of administrative procedure. However, the cuts in social rights have had devastating consequences. The ones who suffer the most are the most precarious fringes of the popular classes, where some people have died of hunger as a consequence of the entry into force of Aadhaar. In addition, the databasing of the population puts public and political liberties at great risk. Apart from the issue of the integrity of personal data that we already mentioned, we should not forget the battle that took place before the Supreme Court. Justice attempted, in vain, to defend the right to

privacy put into question by one the Indian states. This right is however—very—formally acknowledged today. But the fact that a law for the protection of personal data is still in preparation more than ten years after the launching of a programme that is directly threatening the security of private data, reveals the true state of affairs.

Finally, the political situation must not be neglected. Whereas the UID was set up by a progressive coalition, Hindu nationalists are now in power and could well use the capacities of placing the population on file offered by the programme against their opponents. From this perspective, in the "citizens register" that is currently being set up on the basis of Aadhaar, Muslims could well have to prove their nationality.

What would you say as a conclusion? In a few words...

Let us hope that Aadhaar will not serve to illustrate the theory of involuntary effects, i.e., that conceived in an inclusive perspective at best, or purely mercantile at worse, the Unique ID could in fact establish a form of surveillance close to that studied by Michel Foucault for the modern era with the further amplification made possible by the power of IT.

Interview by Corinne Deloy, CERI.
English version by Miriam Périer (CERI) and Caitlin Gordon Walker