Data theft: on UIDAI exposé

Undercover investigations or so-called sting operations occupy a complex and problematical ethical space in journalism, but it is impossible to fault *The Tribune*'s exposé, published after accessing Aadhaar's database of names, numbers and addresses. To begin with, the public interest — which lay in showing how easily the database could be breached and drawing attention to the existence of an organised racket to facilitate this — far outweighed, or more than compensated for, the act of unauthorised access, in this case secured on payment of a few hundred rupees. The investigation was written up in the best journalistic tradition — it focussed on how the data were being mined for money, it did not leak any Aadhaar numbers or other details to establish this, and it sought and received a response from shocked officials of the Unique Identification Authority of India before going to print. So it would have been a travesty of justice if *The Tribune* and the reporter who broke the story were treated as accused in the case where the charges include cheating under impersonation. It would have amounted to more than shooting the messenger. It would have constituted a direct attack on free public-spirited journalism and dissuaded attempts to hold public authorities and institutions accountable for shortcomings and promises.

As for the FIR filed against the journalist, the UIDAI has clarified it needed to provide the full details of the incident to the police and that this did not mean "everyone mentioned in the FIR is a culprit…" In response to widespread disapproval of the prospect of a case being registered against the journalist, the Delhi police have belatedly clarified that they would focus on tracing those who sold the passwords to enable access to the information. Given the noisy hubbub and the misinformation about what was breached, it is perhaps important to stress that the encrypted Aadhaar biometric database has not been compromised. The UIDAI is correct in stating that mere information such as phone numbers and addresses (much of which is already available to telemarketers and others from other databases) cannot be misused without biometric data. The suggestion that the entire Aadhaar project has been compromised is therefore richly embroidered. But even so, it is obligatory for those who collect such information — whether it is the government or a private player such as a mobile company — ought to see that it is secure and not used for purposes other than that for which it was collected. In this digital age, a growing pool of personal information that can be easily shared has become available to government and private entities. India does not have a legal definition of what constitutes personal information and lacks a robust and comprehensive data protection law. We need to have both quickly in place if the Supreme Court's judgment according privacy the status of a fundamental right is to have any meaning.

Rajinikanth is seeking votes as a repository of people's trust, as MGR and Jayalalithaa did

END