DAWN

25th June, 2019

FBR-Nadra portal

HISTORICALLY, tax amnesty schemes haven't had significant success, with those who choose not to document their assets often not taking the bait. Clearly, the government is intent on making its scheme work where others have failed — by swapping the fishing line for a trawler net. In announcing the launch of an online tax-profiling portal with data collated by the FBR and Nadra only days before the June 30 assets declaration deadline, the government's message is clear: they have a detailed picture of citizens' assets, income, expenditures and lifestyles, ie information that can be used in the future to prosecute individuals who have so far evaded the law. However, and perhaps in large part because it took the public by surprise, many have expressed discomfort and anxiety with this rather drastic signalling. And not without reason.

The fact that the decision to upload the personal data of around 53m citizens online was taken without following a stakeholder process and parliamentary debate is quite concerning. The Constitution guarantees citizens' right to privacy, and though the data collected by Nadra, for example, was willingly submitted, it was without the understanding that this information would be put on an online portal at some future date. The fact that travel history is also included in this profile has been particularly jarring for many. In an age when even using a relatively benign app requires consenting to an exhaustive terms-and-conditions agreement, this betrays a lackadaisical attitude towards how Pakistanis' personal data is gathered, stored and used. And though FBR chairman Shabbar Zaidi has given assurances that the database is secure, the general lack of transparency prior to the portal's launch still raises serious questions about what precautions have been taken — or what recourse citizens have in the (however unlikely) event of a security breach. Pakistan still lacks a personal data protection law. A draft bill introduced by the IT ministry last year has several major shortcomings — the most pertinent in this case being that it does not extend to public bodies and government-held personal data, which includes biometric details. Following the June 30 deadline (after which the portal would have effectively served its purpose) it ought to be taken offline. However well-intentioned this initiative may be — and it is hoped that it is successful — security and privacy questions need to be answered before any similar actions are undertaken again.

Editorial