**Fair elections?**

Dr Naazir Mahmood

Monday, Nov 29, 2021

The writer holds a PhD from the University of Birmingham, UK and works in Islamabad.

When our last military dictator General Pervez Musharraf launched the National Database and Registration Authority (NADRA), he made pretty tall claims. One of them was that under the then-new system, forgery of national identity cards would become impossible.

Now the Federal Investigation Agency (FIA) has unearthed a major hacking of the national institution’s biometric data. The FIA has also revealed that some people have managed to export a large number of fake SIMs. This disclosure is not hearsay or rumour; it was discussed in a briefing to the National Assembly Standing Committee on Information Technology and Telecommunication. The officer who made this startling announcement was not a junior officer but an additional director of the FIA Cybercrime Wing. The revelation about the hacking of NADRA’s biometric data is shocking, to say the least.

If NADRA’s system which holds important information can be compromised, what surety there is about the transparency of its system in the next general elections in which the PTI-led government is planning to allow the use of electronic voting machines and online voting by expatriate Pakistanis? Even though officials have attempted to clarify that the hackers have not been able to access all of NADRA’s data, there are serious concerns about how the institution is working and who is responsible for this breach of trust. It appears that during the SIM verification process, which involves biometric data, the system was compromised.

The FIA has claimed that it has seized as many as thirteen thousand fake SIM cards during a crackdown in Faisalabad. This is not a small number, keeping in view that there may be even more fake SIM cards either circulating in the market or being used by someone. Such data breach makes ordinary people highly vulnerable to cybercrimes. There have been many reports that unscrupulous people have duped elderly people and women into giving them their sensitive information – CNIC number, credit card number, etc – and committed financial fraud. In these situations, both the FIA and NADRA cannot do much and usually give the excuse that they are understaffed.

Culprits who carry out such crimes are usually confident that they will get away scot-free. When NADRA started taking the fingerprints of all applicants, a majority of people were against this practice. They cited examples of other countries where such data became vulnerable, but our decision-makers refused to pay heed to that sensible advice. The entire system of NADRA, keeping family trees of each citizen with minute details of all family members, was preposterous from the get-go. It smacked of an authoritarian state that wants to keep an eye on all citizens lest they deviate from the state policy.

There are not many countries that have spent billions in setting up and running an identity mechanism of their entire population. Most countries use other forms of identification such as birth and educational certificates, passports, property documents, utility bills, and other similar papers. Earlier, there was some apprehension that these documents can be forged; now we have evidence that even computerised national identity cards (CNICs) may be fake. The state also has a weapon of ‘blocking’ CNICs whenever it wants to punish or target a particular individual.

In such cases, victims have to approach the court to unblock their CNICs. Sometimes a CNIC doesn’t even help if the fingerprints do not match with the data that NADRA keeps. Now, Pakistan Telecommunication Authority (PTA) Chairman Major Gen (r) Amir Azeem Bajwa has said that some criminals are using ‘illegal methods’ to take people’s thumbprints, and this is why the PTA is phasing out the thumbprint system. According to his statement, the authorities have blocked over 0.5 million SIMs. This is a staggering figure that shows the monumental scale of the failure of our authorities.

One wonders why we are so fond of the term ‘authorities’; housing societies are authorities, Pemra is an authority – so are NADRA, Ogra, and the PTA. If one counts the number of such authorities, they must be in dozens – and look at the quality of work such ‘authorities’ are doing.

The PTA chairman has also recently disclosed that just in October 2021, 26,000 fake SIMs came to PTA’s notice. What about the thousands – or maybe hundreds of thousands – of SIMs that PTA officers were unable to find? When in August NADRA launched a mobile phone application which enabled citizens to use their smartphones for biometric verification, that was perhaps the turning point.

In 2020, there were reports of a data breach involving the sale of 115 million Pakistanis on darknet. This number is equivalent to nearly all of the working population of the country. The government loves to claim that it is keeping pace with technological advancements and wants to enable people to vote through electronic voting machines (EVMs) and online from overseas. The PTI’s digital obsession is not going down well with the Election Commission of Pakistan (ECP) and the civil society and a majority of political parties. Keeping in view the possible intentions of the government to plan for winning the general elections, the introduction of this ‘questionable’ technology is highly controversial.

It will be fairly hard to ascertain the digital identity of voters through machines and online. The way the government has accelerated its move towards new technology that is vulnerable to intentional or unintentional hacking, makes it abundantly clear that the future of democracy is at stake. Not that democracy was safe any other time; it is simply the longest-running democratic cycle that is in danger now. The government claims that the new technology will be a game changer, but the question is: in whose favour?

The government needs to create trust instead of breaking whatever trust people have in the system by moving headlong – as it has done in the recent legislative farce. Democracy is an agreement between the people and the state; this agreement deserves respect. The next elections will see the use of electronic identities which are now under the control of the relevant authorities such as NADRA and the PTA. The government has complete trust in officials who are running these organisations; otherwise they would not be occupying these positions. These identity providers will not be beyond reproach.

Facilitating the verification of CNICs will be an uphill task in a peculiar situation when the systems in Pakistan are prone to failure, especially when you need them the most. For example, CCTV cameras that the state has installed, and controls, tend to fail when there is a breach of people’s rights. The much-touted Pak-ID portal is another example that may turn out to be a portal to benefit those who may want it to work or not work at any time. Just like the RTS did at the most crucial moment in 2018.

The Pak-ID mobile app that Nadra is operating may be a revolutionary step in providing convenience, especially to overseas Pakistan. It may also be a ‘game changer’ in altering election results to benefit certain quarters. It captures documents, fingerprints, and photographs using mobile phones, and at the same time it may be an initiative that may harm the electoral process in the country by manipulating the data it captures – or prefers not to capture – at a certain time. The PM’s vision of a digital Pakistan may turn out to be a vision of digital partisanship.

Email: mnazir1964@yahoo.co.uk