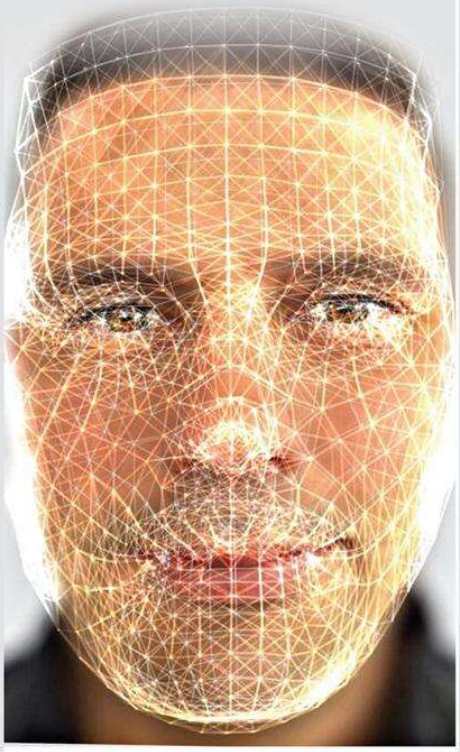
Facial recognition tech: A Damocles' sword spying over our heads



S. Balamurugan, writer and advocate. For contact: balamuruganpucl@gmail.com

The Home Ministry has announced its plan to create facilities for using genetic information collection and facial recognition technologies. The union government has declared that these facilities will be established under the Criminal Procedure (Identification) Act, 2022.

On the one hand, it is said that the fingerprints and genetic samples of the accused will be stored so that in future it is easier to identify the perpetrators of crime. On the other, fears are expressed from several quarters that this move will affect the individual freedom.

Life-long identity

Under the earlier The Identification of Prisoners Act, 1920, judicial permission was required to take fingerprints and photographs of the accused, that too, in the very presence of the judges concerned. But under the present law, powers are vested with the officer of a police station. The technological datasets about the accused will be mobilised from all police stations and stored in the National Crime Records Bureau for up to 75 years. It means that once a person becomes an accused in a case, all information and data about the person will be in storage as long as the person is alive and will be accessed and scrutinised whenever required. The datasets about an accused include the person's fingerprints, leg prints, photographs, signature and iris recognition.

Tamil Nadu Chief Minister M. K. Stalin introduced the facial recognition app in police stations across the state on October 4, 2021. This has been established at airports at the cost of several crores of rupees. In the time of corona, this kind of surveillance became quite natural in the society with the pandemic providing justification. These apps are attached to the surveillance cameras. With the help of this technology, an accused or a suspect can be traced easily, comparing the photograph of the accused already recorded with that captured by the surveillance camera. In most cases, a person's photograph uploaded in the app is downloaded from social media platforms and from some other sources. So, human faces are forced to be exhibited at places fitted with cameras keeping tabs on the people.

Human rights violations

But the catch is that there is no transparency in the way the police use these technologies which are probably prone to errors. Moreover, laws on the use of facial recognition technology and the rules on individual data security are yet to be fully formed. The Information Technology Act, 2000 has no detailed exposition on the use of technology. Under the digital data protection law of 2011 too, there is no security for the personal data collected. Even if rules in this regard are formulated in the days to come, the fundamental feature of human rights violation will remain intact.

In fact, the government has turned a blind eye to the Supreme Court verdict in the Aadhar case (Justice K.S.Puttaswamy (Retd) vs Union of India), which has explained the right to privacy as a fundamental right.

It has not been clearly stated under which circumstances the citizens will be subjected to surveillance by the facial recognition technology. It is not known either why or under what circumstances a person will be suspected. Besides, there is no guarantee that the data collected through technology will be protected from leaking out. Recently it was

reported that the Aadhar datasets about 81.5 crore Indians were stolen and sold in the outside market. This report drives home the danger involved in this issue. Experts have pointed out that the surveillance app has also space for accommodating its makers' whims, fancies, likes, dislikes, bias and partiality. For instance, the technology can be misused against religious minorities or may have the colours of caste or colour discrimination. That is why fears are expressed that the technology will lead to violations of human rights.

Questions afloat

According to the Delhi police, several accused were identified through this technology, who were involved in the riots that broke out close on the heels of the peaceful agitations launched against the citizenship amendment law. They have said that additional face recognition cameras were fitted in the Muslim-dominating areas in Delhi.

But this app has the potential of wrongly identifying the people. In the High Courts in Chennai, Allahabad and Telangana, the affected people have challenged the basics of this technology.

When a democratic society keeps tabs on its citizens through a surveillance mechanism, it certainly trespasses on their individual human rights. A government that always spies on its people is, no doubt, ethically and morally wrong. It means that the people are considered as potential criminals – a highly disturbing irony indeed!

West's stance

Countries such as Italy, Belgium and so on have banned this technology till it is fully guaranteed that it is safe, secure and harmless. Activists have seamlessly been mounting pressures on the rulers to ban this technology across Europe. Moreover, over 24 cities in the U.S. including New Orleans, San Francisco and Boston have already banned this surveillance app. Over 180 organisations including the International Human Rights Commission have alleged that this technology flouts human rights and international human rights laws, targeting the alternative political ideologues. Several software corporates, in view of the mounting global opposition, have announced not to develop the technology any longer.

The government should respect and uphold the people's fundamental rights and democratic values. It will do well to keep in mind that bringing all people under scanner

always is utterly erroneous for it militates against the basic democratic structure of the country.

Translated by V. Mariappan.