International Politics and Society

Data protection is social protection

Worldwide, governments and corporations collect private data from beneficiaries of social programmes. They need protection

By Magdalena Sepúlveda | 19.04.2019

An election official scans a voter's eye with a biometric device at a polling station during a parliamentary election in Kabul

In recent decades, social assistance programs around the world have been strengthened to the point that they now benefit more than 2.5 billion people, usually the poorest and most vulnerable. But rising pressure to apply biometric technology to verify beneficiaries' identities, and to integrate information systems ranging from civil registries to law-enforcement databases, means that social programs could create new risks for those who depend on them.

Private companies, donor agencies, and the World Bank argue that the application of biometric tools like iris and fingerprint scanning or facial and voice recognition, together with the integration of databases, will boost efficiency, combat fraud, and cut costs. And many governments seem convinced.

While there is no systematic information available on the use of biometric technology in social-assistance schemes, a look at certain flagship programs suggests that it is already on the rise. In South Africa, 17.2 million beneficiaries of social grants receive biometric smart cards. In Mexico, the 55.6 million beneficiaries of *Seguro Popular* (public health insurance for the poorest citizens) must provide their biometric data to the authorities.

The world's largest biometric database – Aadhaar – is in India. Because inclusion in Aadhaar is a prerequisite for access to several social programs, 95 per cent of the country's 1.25 billion inhabitants are already recorded. The provision of biometric data is also required to receive benefits in Botswana, Gabon, Kenya, Namibia, Pakistan, Paraguay, and Peru.

The risks of disclosing social-protection data

Biometric data stored in one social-protection program database can easily be linked to other systems using a common identifier, even those unrelated to social protection, such as for law enforcement or commercial marketing. In most European countries, however, such database integration is prohibited, owing to the threat it poses to privacy and data protection. After all, social-assistance programs require the processing of significant amounts of data, including sensitive information like household assets, health status, and disabilities.

In many of the developing countries that are expanding their social-protection and biometric-identification programs, the frameworks for protecting personal data are underdeveloped. Yet donors and government authorities often advocate the widest possible integration of databases, among public and private entities alike. For example, Nigeria, which aims to issue 100 million biometric e-ID cards, has a National Identity Database connected to various other databases, including those maintained by law enforcement agencies.

Pressure to share sensitive social-protection data, including biometric identifiers, with law enforcement – domestically, as well as internationally – is compounded by concerns about terrorism and migration. This pressure threatens not only basic privacy, but also civil liberties. Add the risk of negligent data disclosure or unauthorised third-party access – including by cybercriminals and hackers – and social-protection beneficiaries could also be exposed to stigmatisation, extortion, or blackmail.

Social-protection programs are supposed to do just what the name implies: protect those segments of society that are most in need.

Then there is the possibility that access to sensitive social-protection data, including biometric information, will be given or sold to private companies. Social-protection authorities and private companies, such as MasterCard or Visa, frequently enter into commercial agreements to create smart cards for social-assistance programs or to arrange for businesses to accept those cards. For example, South Africa's social-assistance biometric card is a MasterCard.

Worse still, such agreements – which often are not publicly disclosed – tend not to include mechanisms for redress in cases of abuse and misuse of information. Yet recent media reports suggest that these risks are considerable. For example, in Chile, millions of patients' medical records – including those of HIV patients and women who had been sexually abused – were publicly exposed for almost a year.

Moreover, in South Africa, private companies used the information of millions of social-protection beneficiaries to increase corporate profits to the detriment of beneficiary interests. In India, a newspaper claimed that its reporters had gained unrestricted access to the Aadhaar database. Another report documented how Aadhaar numbers, with sensitive financial information, had been made publicly available on government websites.

Lobby for data protection

The threat to social-protection beneficiaries is not eliminated even when data are accessible only to government. As the political scientist Virginia Eubanks recounts, in the United States, automated decision-making in social-welfare provision enables the government to 'profile, police, and punish

poor people.'

As technology continues to advance, these threats will only grow. For example, facial-recognition technology may enable governments to identify protesters who receive social assistance using the digital photographs they have provided in exchange for access to benefits. Malta, for example, is already considering using CCTV cameras with facial-recognition software to prevent 'antisocial behaviour.'

The lack of regard for privacy and data protection in social-assistance programs should not come as a surprise. These programs serve the most vulnerable groups – people who are already at a disadvantage in defending their rights. Entrenched stigma and anti-poor prejudices often prevent other, more privileged members of society from recognising those risks, much less advocating on behalf of social-protection recipients. Many seem to believe that if you are receiving 'free' benefits, you cannot also demand privacy.

Social-protection programs are supposed to do just what the name implies: protect those segments of society that are most in need. Demanding that these people effectively renounce their rights to personal privacy and data protection amounts to just the opposite.

That alone should be enough reason to lobby for the adoption of adequate legal frameworks, well-resourced data protection authorities, and, as a last line of defence, an independent judiciary and media. But if people need a stronger incentive, there is always self-interest, because the risks faced by the most vulnerable and disadvantaged today may well become reality for a much broader cross-section of society tomorrow.