EGM/B+25/EP.11

September 2019

ENGLISH ONLY

UN Women

Expert Group Meeting

Sixty-fourth session of the Commission on the Status of Women (CSW 64)

'Beijing +25: Current context, emerging issues and prospects for gender equality and women's rights'

New York, New York

25-26 September 2019

The use of biometric technology in social protection systems. A gender perspective

Expert paper prepared by:

Magdalena Sepúlveda Carmona*

Global Initiative for Economic, Social and Cultural Rights, Mexico

* The views expressed in this paper are those of the authors and do not necessarily represent those of the United Nations.

Abstract

In the past decade there has been an increased use of biometric technology in the identification and authentication of beneficiaries of social protection programs. However, there has been little debate among governments, donors and civil society organizations on the potential implications for gender equality or for the enjoyment of other rights, such as personal security and the protection of privacy and personal data. These are considerable gaps. Considering that women are most of the beneficiaries of social protection programs the existing lack of gender analysis is at least negligent. Is the use of biometric technology in social protection programs increasing the exposure of women to threats to their integrity and rights?

Technology's rapidly expanding power is giving rise to a range of new threats, including covert surveillance on program beneficiaries. For example, advancement in facial-recognition technology may allow identifying protesters through the digital photographs they have provided to a social protection program. Mass information collection also encourages cybercriminals and hackers to undertake sophisticated scams.

First, the paper reviews how biometric technology is used in various social protection programs around the world. Then, it examines the potential risks and challenges of deploying biometric technology in social protection programs. Finally, it assesses the requirements necessary to ensure that biometric technology is implemented in compliance with international law standards including gender equality. The focus is on the potential risks for women and girls. Among the key conclusions of the paper is that adoption of biometric technology should be accompanied by a context-specific assessment of risks, and the adoption of an appropriate legal and institutional framework to protect rights and ensure that women as well as the most vulnerable and disadvantaged members of the population are not excluded or disproportionately impacted.

I. How biometric technology is used in social protection programs?

While there are various ways in which biometric identification systems, mainly fingerprinting, iris and facial recognition, are used in social protection programs, in most cases, they are involved in identification and payment systems (or a combination of both), and sometimes the monitoring of conditionalities (co-responsibilities).

Biometric systems have been used in a variety of context in programs of different size. Examples of cases include the following:

Collection of biometric data

The first part is to capture the biometric data as part of the enrolment process. Individuals are required to submit to a digital recording of biometric identifier such as fingerprinting, iris or facial. Usually, once such information is captured, each recipient receives a smartcard.

Storage

Once the biometric has been collected, it is stored in a centralized database and/or in a smartcard which contains a chip that holds the biometric information previously taken from the holder. In some cases, such

as in South Africa, in addition to the biometric information, the smartcard holds information on the individual's grant, including payment schedule, amount, and date of late payment received. Having this information on the smartcard allows the system to operate offline (Gelb and Decker, 2011).

De-duplication and Authentication

When the information has been collected and stored, it could be compared with other templates to ensure it is unique (de-duplication), and it can also be used for authentication (verification). The biometric information establishes the uniqueness of every individual. For example, a beneficiary of social protection programme may authenticate his/her fingerprint against a template stored on a smartcard, on a database or in a point-of service (POS). Both de-duplication and authentication require comparisons between an enrolled biometric and a stored template.

To verify identity for payment or service

Individuals registered in the programme identify themselves with their fingerprints or iris to receive the payment or service. Often, at the time when beneficiaries go to a pay-point they are required to present a card as well as fingerprint for biometric identification in order to take the cash.

To record and verify compliance with conditionalities

Biometric technology has also been used to verify compliance with transfers' conditionalities in some cash transfers programs. In such cases a stand-alone fingerprint biometric machine is installed in schools and/or medical centers for recoding school attendance and mother's visits to health clinics.

While information on biometric technology use in social protection programs is not systematically available, an examination of certain flagship, non-contributory programs suggests that in recent years developing countries have increasingly used biometric systems to identify programme beneficiaries *(who are you?)* as well as authenticate the identity of those beneficiaries *(are you who you claim to be?)* upon delivery of payments/services. The trend suggests using this technology in social protection programs will continue and probably increase.

The South African Social Security Agency (SASSA) has a large biometric database as social grant recipients receive biometric smart cards – *SASSA Debit* MasterCards for which their fingerprints, photographs and even voices are captured (SASSA, not-dated). By March 2018, there were more than 17.5 million grant beneficiaries (SASSA, 2018). In Kenya, beneficiaries of the *Hunger Safety Net Programme* (HSNP) receive a smart card with fingerprint information and an identifying photograph. In Botswana, food-grant recipients receive a smart card called *SmartSwitch* which contains beneficiaries' personal details and fingerprints. In Namibia, social protection beneficiaries receive a smart card called the *Epupa* card. Beneficiaries insert the *Epupa* card and present fingerprints for biometric identification to receive their cash.

In Mexico, the healthcare initiative to the population's poorest segments, *Seguro Popular,* issues biometric card to each beneficiary family. The system captures all fingerprints of each member of the family above 10 years of age. In 2016, 55.6 million people benefited from Seguro Popular (CONEVAL, 2018). Similarly, in Gabon, a health insurance for those living in poverty - the *Gabonais Economiquement Faibles*- also uses biometric ID cards and serves 417,118 people as of 2011(WHO, 2013). In both cases,

fingerprints confirm the identity of the biometric ID card's bearer before he or she can access governmental services or healthcare.

In Peru, beneficiaries of the Conditional Cash Transfer (CCT) *Juntos* receive a biometric smart card called *Multired*. Moreover, biometric technology has been used to monitored compliance with conditionalities (i.e. co-responsibilities). Biometric technology has also been used to monitor compliance with conditionalities (co-responsibilities). A pilot programme used a fingerprint biometric system to check children's school attendance. Schools had digital fingerprint readers and children were required to present fingerprints as proof of attendance (Gobierno Peru, 2018).

One of biometric technology's most representative uses occurs within India's Aadhaar programme. This programme gathers "demographic data" (i.e. name, gender, date-of-birth and residential addresses, and, optionally, mobile phone numbers and e-mail addresses), as well as "biometric data" (i.e. ten fingerprints, both irises plus a digital photograph) to identify beneficiaries when they access social benefits and government welfare programs. After a free-of-charge enrolment process, beneficiaries receive a twelve-digit, randomly generated "Aadhaar number" that India's Unique Identification Authority (UIDAI) issues.[1] Aadhaar is the world's largest biometric database, covering over 90 percent of India's 1.25 billion inhabitants (Mukherjee, 2018).

Biometric systems are also increasingly used in humanitarian settings. For example, the United Nations Hight Commissioner for Refugees has a Biometric Identity Management System (BIMS) that records fingerprints and iris scans of large numbers of refugees in several operations. According to UNHCR while overall there seems to be equal numbers of men and women refugees, in some regions, such as sub-Saharan Africa there is a higher proportion of women (52%) than men (UNHCR, 2019).

II. Risks and challenges in the use of biometric technology in social protection

There are merits of improving identification in social protection programs. However, there are also risks to the enjoyment of human rights that policy makers, donors and the general public should be aware of to be able to better assess and evaluate the various options for identification in social protection programs.

While these risks impact men and women, due to structural discrimination women are more likely to be living in poverty, more likely to be living in families with dependent children and more likely to be lone parents. As a result, they are most of the beneficiaries of social assistance programs. For example, in Brazil, in 2010, 94% of beneficiaries of the CCT, Bolsa de Familia, were women (Holmes et al., 2010). However, despite this there has been little research to date into the specific impact of the use of biometric technology in social assistance programs and even less on the gender impact. This is a major gap, considering that women are likely to have a disproportionate impact.

This section classifies the risks in 5 broad categories:

[1]Information retrieved from the UIDAI website at https://uidai.gov.in/your-aadhaar/about-aadhaar.html [2 May 2018].

(1) Inaccuracy of data; (2) Identity theft; (3) Exclusion; (4) Security risks and misuse of the data and (5) Data-Sharing between databases.[2]

Policy makers, donors and the general public should be aware of the risks to be able to better assess and evaluate the various options for identification in a social protection program.

1. Inaccuracy of data

Despite the rapid advancement in biometric technology, its use is not exempted from failures. First, the biometric data contained on a smartcard and on a national database is only as reliable as the original scanning –whether manual or automated- and only as secure as the trustworthiness of the officials or private contractors charged with this task (Breckenridge, 2005).

Second, there are several failures that may occur when individuals enroll their biometric data and during the process of matching an individual's biometric against a template stores in a database (ISPA, 2016):

- Fail to enroll: the hardware cannot capture an imagine of high quality;

-False positive: the system erroneously finds a match between the captured biometric and the stores template; and

-False negative: the system erroneously finds no match between captures biometric and the stored template).

In Kenya, for example, difficulties with reading around 5 per cent of all fingerprints have been reported in relation to the HSNP programme smart card payment system, due to technical difficulties sometimes related to very old or worn-down finger pads (Harvey et al., 2010). Older people's fingerprints were often illegible in Namibia and led to proxies receiving cash on their behalf, with the consequent risks this entailed (ILO and Oxford Policy Management, 2014).

Third, there may be technical problems with the specific card, such as micro-chips in smartcards not working or fingerprint scanners not able to verify for several reasons. While the precise consequences of these errors are not the same, from a rights perspective, emphasis should be placed on ensuring that people are not prevented from accessing social protection programs or receiving the benefits that they are entitled to. In this sense, if a trade-off between false acceptance rate and false rejection rate needs to be made, from a rights perspective the latter should be minimized. The enrolment errors or false negative errors should never lead to the automatic exclusion of a person from benefiting the programme; instead errors should be properly addressed by programme staff without placing a major burden on the beneficiary. For example, a mismatch between the fingerprints of the holder of a card and the biometric in that document should draw the competent authorities' attention to the person concerned who should then seek an alternative check of that person's identity without preventing the person from accessing the payment of benefits.[3]

[2] Some of these risks are not specific to the use of biometric technology as they could arise with low-tech identity solutions. Still, the use of biometric technology might exacerbate them.

[3] This is in fact the standard established by the European court of Justice regarding biometric passports. See, Michael Schwarz v. Stadt Bochum, Case C-291/12, judgement of the European Court of Justice, 17 October 2013. Available at: http://curia.europa.eu/juris/document/document.jsf?text=&docid=143189&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=514948

2. Identity theft

Considering that biometric can link an individual to an identifier in a way that other methods cannot do, the use of biometric will make some forms of identity theft harder. Nonetheless, it would be a mistake to assume that they provide full guarantee against or prevent identity theft.

A major disadvantage of the biometric technology is that once the identifier indicators are compromised, they cannot be reissued like signatures or passwords. Fingerprints or irises cannot be reissued when imposters gain access to this data. Ultimately real beneficiaries are hard pressed to re-claim their identities and access the money or essential services upon which subsistence depends. While incentives for identity theft to defraud social protection programs may be limited, acquiring new identities can be of vast interest to those who would pose as others when arrested or when they seek to obtain medical care, medicines, credit, goods and services.

When chip-cards with biometric information are stolen, the failure to present the card should not lead to the denial of the payment/service. To prevent excluding those most in need, a system should be in place to ensure that people whose cards had been stolen (or even lost) could still receive services while waiting for a replacement. Moreover, the costs for the replacement of cards should not be punitive. A card replacement should be accessible for the most vulnerable even in the event of negligence. If such systems are not in place, there would be additional exclusionary factors.

3. Exclusion

Any administrative requirements for identification, registration and payment methods should consider the special needs of women and other vulnerable groups such as children and older persons. Lack of adaptation to their needs could represent the difference between inclusion in and exclusion from social protection programs.

Due to structural discrimination, women might be disproportionately excluded from a social protection program when biometric systems are in place. The situation will be exacerbated when gender intersect with other inequalities such as race, disability and age.

There are several factors that might prevent women from benefitting from a social protection programme when biometric identification systems have been requested (see textbox).

Textbox

Potential exclusionary factors

- Lack of awareness of the enrolment process or information about the importance of enrolment;
- Limited infrastructure/presence of the enrolment office/station;
- Not being reached by the system: limited physical mobility, safety concerns and inadequate transport and infrastructure facilities that prevent the person to reach the place where s(he) has to provide biometric information;
- Inability to pay for the identification card or any other administrative requirement;
- Physical inability to provide a reliable biometric information;

- Cultural barriers, mistrust and stigma that prevent enrolment; and
- Gender social norms and patriarchal attitudes that exclude women.

Source: author's elaboration

When designing the identification process, policy makers should be cognizant of the specific needs and interests of women, and the diversities among different groups of women. In patriarchal societies, social norms and gender stereotypes construe women as second-class citizens whose place is in the home while male is seen as "head of household" representing his family and community. Therefore, unlike men, it is assumed that women do not require identity documents. This would indicate that even in aspects regarding women's right to have identification documents, decisions would be taken with and by others as spouse, parent and/or siblings.

Therefore, women are often less likely to be registered than men. In Pakistan, since 2000, the National Database and Registration Authority (NADRA) has taken specific measures to increase access by women to the Computerized National Identity Cards (CNIC). A critical tool to reach women has been the implementation of the so-called Mobile Registrations Vans (MRVs) [4]. Still, in 2009 only 64 per cent of women over 18 years old had a biometric identity card in comparison with 95 per cent of men (Hakeem, 2009). Moreover, an assessment by World Vision in 2012 found that in a flood affected village more than 30 per cent of the community did not have a CNIC, of which 70 per cent were women. While it was found that women were generally not aware of the importance of having a national ID, there was also a problem of distance: reportedly the nearest NADRA office was located at 35 km and the villagers. Women were more likely unable to hire a motorbike for the two hours bike ride.[5]

The choice of identifier should also be gender sensitive. It has been argued, for example that iris scan may be more culturally acceptable for women in Muslim communities as there is no physical contact and practically feasibly in places where women wear a burqa (Gelb and Decker, 2011). Cultural norms of indigenous women and ethnic minorities might prevent them from allowing to be photographed (Gellman, 2013).

The enrolment staff should also be sensitive to the multiple forms of discrimination that might arise at the intersection of gender, age, race, class, disabilities, etc. For example, even when beneficiaries or potential beneficiaries speak the predominant language in a country, cultural differences (alongside the imbalance of power) can impede communication between the program's official and those seeking for registration/enrolment. For example, in Peru, the problems of cross-cultural communication between the indigenous peoples and civil registry officials, have been considered as one of the causes for the lack of registration, as well as sources of errors or omissions in the registration of birth certificates (Peru, Registro Nacional de Identificación y Estado Civil, 2012).

[4] Information retrieved from Pakistan National Database and Registration Authority (NADRA) website. Available at: http://www.nadra.gov.pk/index.php/about-us/profile

[5] Information retrieved from World Vision Pakistan website. Available at: http://www.wvi.org/pakistan/article/new-life-id-cards

To ensure inclusiveness the training of programme staff should go beyond the mere technical aspects of the use of biometric technology. They should also have the capacity to enroll or verify identity in a way that respects the cultural differences and is gender sensitive. This type of training in staff capacity requires additional investments and stability in the types and level of functions carried out by staff.

Since its establishment, India's Aadhaar programme has been strongly criticized for various reasons, including for not adequately reaching the nation's most vulnerable groups and violating privacy rights (see, for example, Ramanathan, 2014). A landmark Indian Supreme Court ruling from 24 August 2017 asserted the right to privacy is a fundamental under the Indian constitution, intrinsic to the "right to life and personal liberty" (Supreme Court of India, 2017). The case dealt with a batch of petitions challenging government moves to make Aadhaar mandatory for accessing several social welfare programme benefits.

4. Security risks and misuse of data

Any identity registry might attract abuses in particular when it contains highly sensitive information. Recent history reveals several examples of abuses of registries such as the use of the Dutch population registers by the Nazi regime to persecute Jewish families (Moore, 1997) and the role of identity cards in the Rwanda genocide (Longman, 2001). Even during peacetime, identity registration has been used by governing authorities to control the movement and liberty of sections of their populations, for example in South African apartheid and tsarist and soviet-era Russia (Setel, 2007). When personal information is collected and storage through electronic tools (i.e. a database and not just a written record), these risks are increased.

The collection, storage and processing of personal data raise innumerable risks of violations of rights. On the one hand, there are risks related to the protection of personal data such as loss or unauthorized access, destruction, modification or disclosure of data. 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 (CIPER, 2016). On the other hand, there is the potential of misuse of the information by the Governments or the private sector for systemic surveillance of individuals, interception, data collection and commercial purposes. Moreover, any information resource maintained in computers connected to the Internet may be targeted by Internet espionage including by private companies.

Currently, States have a greater capability to conduct simultaneous, invasive, targeted and broad-scale surveillance than even before, and biometric technology greatly facilitates this type of intrusions (OHCHR, 2014). Biometric information can provide identifiers across systems and even across borders, tracking individuals in all contexts, allowing for the reuse of the information and making sharing, linking and cross-checking information faster (Hosein and Nyst, 2013).

The rapid way technology develops also raises concerns about the particular risks of some biometric technologies, and the retention of biometric data. For example, the use of digital photography in some programs poses high risks as facial recognition technology is developing quickly allowing for remote surveillance even without the consent of the subject. Quick technological developments are often not matched by legal regulations and ethical frameworks which might come too late. For example, advancement in facial-recognition technology may allow identifying protesters through the digital

photographs they have provided to a social protection program. Malta, for example, is considering using CCTTV cameras with facial recognition software to curb anti-social behavior (Mayhew, 2018). The use of this technology is particularly worrisome in the context of the ability of governments to curtail rights such as freedom of assembly and expression through the identification of protesters.

Due to the development of new technologies, collected biometric information can be re-used for a variety of purposes unforeseeable at the time of their collection. Thus, the development of strict retention policies (i.e. for how long biometric information would be retained) are critically important and should be precisely defined in advance.

By its own nature, database that contains information regarding beneficiaries of social protection programme contain highly sensitive personal information, and thus should follow strict confidentiality standards. Disclosure of the information contain in this type of databases can prompt stigmatization and other forms of discrimination as well as expose beneficiaries to risks in their personal security.

A critical issue in the design of an information system to be used in social protection programs is the type of data which would be included. Some threats to personal data could be avoided by not including certain information in the system or by establishing strict rules limiting data retention and clearly defined accountability lines. The risks increase if certain type of information such as religious affiliations, racial, ethnic or linguistic origin is also collected. The data associated with each of these characteristics may be used for political purposes or to limit or remove rights. For example, political manipulation can occur by targeting disproportionately for transfer a specific influential ethnic group while systematically excluding an ethnic group that opposes the Government (Devereux and Vincent, 2010).

5. Data-Sharing between databases

A critical issue with using biometric technology in social protection systems is the irrevocable link between biometric traits and the creation of an individual's ongoing "dossier". Biometric data stored in information systems can be easily linked within a social protection system or across systems – even with those not related to social protection, such as law enforcement or commercial marketing systems. The aggregation of individual information records in various information systems – and the potential for linking those records through a common identifier – raises several risks associated with data abuses especially in countries without well-developed legal and institutional frameworks to protect rights, personal data, and privacy.

Recent years have seen increased interest in coordinating and harmonizing social protection programs. Integrating social protection data leads to a more effective management of the programs. However, sharing information included in social protection databases across various public or private databases not strictly related to social protection is risky and should be regulated by law and subject to oversight. In principle, information collected for social protection purposes should only be used for social protection purposes. While information integration beyond the social protection sector might seem an appropriate way to increase coordination and enhance efficiency in the use of resources, it may imply data-privacy and -security breaches that must be assessed from the outset.

At the European level, for example, to protect privacy and personal data, most countries do not allow for the integration of different databases. In contrast, in some developing countries where identification efforts have been recently undertaken, donors and government authorities often encourage (or actively

support) the widest possible integration of national identity databases, not only among public organs but also with private entities.

Human rights and data protection concerns will emerge depending on which databases are linked, who accesses data and whether appropriate mechanisms and protocols to protect privacy and personal data are in place. Linking information about social protection beneficiaries to a tax payment database might be justified by an objective of improved targeting and fraud elimination. However, integrating social protection databases with law enforcement registries (e.g. national and international policing agencies) – even when legally authorized and justified on national security and counter-terrorism grounds – is likely to be arbitrary (i.e. the resultant limitation of rights may be disproportionate to programme goals, unnecessary in democratic societies or simply discriminatory).

Global terrorism threats and increased migration exert pressure on national authorities to share citizens' personal information. If such pressure leads to integrating social protection and law enforcement system databases – as some donors propose (World Bank, 2015)– beneficiaries' privacy and data protection rights could be severely curtailed. Moreover, using social protection information for counter-terrorism measures or restrictions in population movements, could lead to distrust of the system and deter eligible participants from applying to much-needed programs.

III. How to ensure that the use biometric technology is gender sensitive?

While there are advantages in the use of biometric technology and in the harmonization of databases to improve the efficient delivery of social protection programs, it is concerning that the implementation of such technology is undertaken without due safeguards to prevent, protect and remedy violations of rights and without a gender analysis.

States must put in place several safeguards to ensure that the use of biometric technology in social protection schemes is gender sensitive and in compliance with international human rights standards. To this end, States should:

1. Carry our assessments of the potential gender inequality impact of the use of biometrics

Implementing a biometric system in social protection programs without sufficient assessment of risks and a gender equality impact could defeat the purpose of the social protection system.

2. Ensuring that the system is inclusive

The use of biometric technology in social protection systems should be adapted to the needs of women and other disadvantaged groups. Cost and other barriers should be minimized to ensure inclusion of those members who might experience greater difficulty in accessing or adapting to the use of such technologies. Moreover, specific safeguards should be implemented to ensure the respect of rights and fundamental freedoms and gender equality.

The assessment of the inclusiveness of a given biometric identification system implemented in a social protection programme should look beyond the specific programme. Inclusiveness in the programme requires a comprehensive set of measures aimed at ensuring access to legal documentation by women and disadvantaged groups. National documents such as birth certificates or national IDs are often critical documents for accessing social protection programs, therefore measures should be taken to bring

national registries closer to the most excluded. This means, for example, that birth registration should be free, simple and available at the local level.

Gender inclusive social protection programs are those that have enabled multiple avenues through which individuals can register, allowing prospective registrants to select the method that is easiest and cheapest for them. Some include mobile registrations units and/or door-to-door outreach as well as integrating registration into other services such as in hospitals, reproductive health services, vaccination programs, and local stores.

It is also critical to provide training -for staff of national registration offices as well as the staff enrolling beneficiaries- in all technical skills in registration matters as well as on issues regarding gender mainstreaming and cultural diversity.

3. Establishing accessible and effective complaints and redress mechanisms

The presumption that biometric technology is infallible makes the establishment of redress mechanisms essential. As the failures in biometric technology become more exceptional, individuals might have more difficulties to challenge failures such as mistaken identity or failure to enroll. Therefore, clear mechanisms and standards for resolving errors and identity disputes should be in place.

Considering that a proportion of the population might not be able to enroll in a biometric system for different reasons or would have problems when requesting payment/services, the system should put in place an appropriate fallback procedure in every stage (from collecting date to accessing services). Such mechanisms should be accessible and well-resourced so women and men who are unable to complete the enrolment process successfully or to receive payments, should not be burdened with the imperfections of the technical system, and their rights respected.

4. Ensuring transparency and access to information

All social protection interventions should have the mechanisms in place to ensure transparency and access to information with respect to all core components of the programme, this include identification and registration processes. Considering that the use of biometric technology in social protection programs is often the result of collaborative efforts of various stakeholders such as donors, governments, NGOs and the private sector, the information about the various roles and responsibilities should be open to public scrutiny.

A lack of transparency on issues related to biometric technology and the collection, storage and processing of personal information may generate mistrust and low levels of public support for a programme.

5. Ensuring women's participation in the design of the systems

Critical decisions regarding the use of biometric technology in social protection systems, such as what type of biometric identifier should be used, what information should be collected and storage, and what databases should be linked must be taken with active participation of women. To this end women should have information about the system, opportunities to clarify doubts and misconceptions and to participate safely.

6. Adopting a legal framework for privacy and data protection

The use of biometric technology in social protection systems makes essential to ensure privacy and protection of personal data against any misuse and abuse (Sepúlveda, 2018). Authorities must take all necessary measures to secure personal data, particularly when processing highly intimate and sensitive data.

Even when countries have data protection laws, State must adopt specific regulations on data protection applicable to social protection systems. This could be done, for example, by:

(a) developing sector-specific data protection policies. Enacting data protection policy applicable to the social protection system would facilitate consistency in the implementation of the data protection legislation throughout all social protection programs within a country.

(b) developing data protection guidelines which would complement policy and facilitate implementation. In Ireland, for example, the Department of Social Protection has developed a Data Protection Policy together with detailed guidelines, to ensure that all staff and others who process personal data on behalf of the Department are doing so in accordance with the principles contained in the national Data Protection Acts.

The legal framework for the protection of privacy and data protection in social protection should enforce the relevant "information protection principles"[6] examined below:

Limiting the collection of personal data ("Collection Limitation Principle")

A practical way to reduce the abusive use of personal data by Governments or third parties is to limit and reduce the information that is collected by keeping it to the minimum necessary.

Collecting the minimum amount of data would not only help protect beneficiaries' rights, but it will also decrease the cost of the system. When developing countries are seeking to implement an identification system for beneficiaries of social protection programs, policy makers should assess and being able to reasonably justify each of the data elements to be included in the system. Ideally, there should be an open and public debate about the data element selected by them before the final decision is taken. All data should be obtained by lawful and fair means.

Ensuring quality and relevance of data ("Data Quality Principle")

The collection and storage of data of the beneficiaries or potential beneficiaries of social protection programs should be limited to those strictly relevant to the purposes for which they are to be used. Moreover, to the extent necessary for those purposes, should be accurate, complete, and kept up to date.

Specifying the purposes for the collection of data ("Purpose Specification Principle")

[6]OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data provide the most commonly used privacy framework; they are reflected in existing and emerging privacy and data protection laws and serve as the basis for leading-practice privacy programmes and additional principles. Other instruments include, the United Nations Guidelines for the Regulation of Computerized Personal Data; the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CoE Convention No. 108) and the EU Data Protection Directive (Directive 95/46/EC). These principles can be formulated in different ways, but the content of various versions remains the same

Individuals should be informed about the intended purpose and the reason why the data has been requested. The purposes for which personal data are collected should be explicit, legitimate[7] and specified at the time of data collection, and subsequent uses should be limited to the fulfilment of those purposes. Ensuring access and control to personal data ("Individual participation principle").

Ensuring participation ("Individual Participation Principle")

Biometric information is a type of personal information critically linked to one's identity therefore, human rights standards plays a critical role in guaranteeing that individuals are entitled to keep this information under their control. Accessible mechanisms should be put in place allowing individuals to know which personal data has been collected and storage, to request corrections and deletion of data in their names at any point.

Limiting the use of the data ("Use Limitation Principle")

Personal data should not be disclosed, made available or otherwise used for purposes other than those specified at the time of data collection. The use of personal data for a purpose not originally intended should require the consent of the data subject or authorized by law. This means, for example that the fingerprints provided to enroll in a social protection programme should be used only for verifying the identity of its holder, and that the fingerprints data will not be read by unauthorized persons.

In social protection programs the "use limitation principle" is also related to any other linked databases. As discussed above, in principle, information collected for social protection purposes should be only accessed by social protection authorities, any exception should be authorized by law. In any case, sharing information of beneficiaries should be done only when it is strictly necessary, on the basis of full transparency, with the consent of the beneficiary and with well-established accountability lines.

A public debate on critical questions, such as what information should be shared and with whom, when are linkages are appropriate and when do they infringe privacy and threaten personal security, might help in building support for the implementation of specific features of a social protection programme. The onus should be on the social protection authorities to demonstrate that any linkages of databases is legal, necessary and proportional to the end goal, and fully in line with the purposes of the programme/system. There should be in place meaningful and proportional sanctions in the case of any contravention.

Safeguarding the data ("Security Safeguarding principle")

Personal data should be protected by reasonable security safeguards against all type of risks including loss, unauthorized access, destruction, misuse, modification or disclosure of data. While risk assessments for government and private databases containing personal information is often a standard procedure in some developed countries, this is not the case for the great majority of developing countries which lack laws and security information mechanisms.

To ensure that the processing and storage of biometric data in social protection programs will be effectively protected from misuse and abuse, policy makers should take a comprehensive set of measures from developing secure physical and digital structure infrastructure to strictly limiting who has access to the information.

[7] See EU Data Protection Directive 28.

Ensuring the necessity and proportionality of the processed data

Biometric data should only be used if adequate and relevant and should not be excessive. There should be proportionality between the use of biometric system and the intended purpose. To ensure compliance with this requirement, a prior assessment should take into account, as a minimum, the following factors: (a) whether the system is necessary to meet the identified need, i.e. it is essential for satisfying the need rather than just being the most convenient or cost effective; (b) whether the system is likely to be effective in meeting that need; (c) whether the resulting loss of privacy is proportional to any anticipated benefit - if the benefit is relatively minor, such as an increase in convenience or a slight cost saving, then the loss of privacy is not appropriate; and (d) whether a less privacy intrusive means could achieve the desired end (Data Protection Working Party, 2012).

Establishing accessible accountability systems ("Accountability principle")

Social protection programs should have simple, effective and accessible mechanisms to submit and process complaints, and provide access to effective remedies in case rights are violated. Such mechanisms should also address issues of privacy and protection of personal data.

The establishment of independent oversight and monitoring mechanisms to ensure accountability of those collecting, processing and storing of information regarding social protection beneficiaries is critical to achieving effective accountability. Any oversight mechanism should at a minimum, provide due process guarantees and being able to offer the deletion of data or other type of reparation. Additionally, consultation with all relevant stakeholders (e.g. social protection authorities, scientific and technical communities, the business sectors, academics, human rights experts) including the program's beneficiaries should be an essential element of any oversight mechanism.

While the adoption of a legal framework securing the principles indicated above is the bare minimum, it is not enough. From a human rights perspective, social protection implementers are obliged to adopt practical and effective measures to prevent abuses on the first place. These include establishing well-resourced data protection authorities and the existence of an independent judiciary and media. When these factors are missing, the risks of disclosure are even higher.

IV. Final Observations

In recent year, the political commitments in expanding social protection programs have been accompanied by the use of new technologies that have the potential to improve the administration of such programs as well as the experience of beneficiaries. This is particularly the case in the use of biometric technology in the identification, registration and authentication of beneficiaries. However, the use of this technology may also exacerbate gender inequalities, negatively impact the rights beneficiaries, and become a major threat to privacy and data protection. Despite that women are more likely to be beneficiaries of social assistance programs, hence disproportionately impacted by this technology, there is little research about the gender impact on the use of this technology.

Unfortunately, the establishment of biometric systems in social protection programs is often not accompanied by serious analysis about their potential negative impact, and thus are implemented without a robust regulatory framework and appropriate levels of physical, administrative and technical security measures and proper accountability mechanisms.

When biometric technology is implemented without a proper gender impact assessment, there are high risks of exclusion: women otherwise eligible may be overlooked or unable to enroll. Moreover, they will be further expose to personal security risks as well as threats to privacy and data protection. These risks imply that there might be tensions between the use of biometric and the main objectives of social protection programs, which is to provide protection to those in need.

References

Mukherjee (2018): "India's Supreme Court Ruling on Privacy and What It Means for Aadhaar," blog post, 8/24/17. Available at https://www.cgdev.org/blog/indias-supreme-court-ruling-privacy-and-aadhaar [2 May 2018].

Hakeem, Ali (2009): "Smart National Identity Card in Pakistan", Poverty Reduction and Economic Management Knowledge and Learning Forum, World Bank, Washington, DC. Available at: http://siteresources.worldbank.org/EXTSAFETYNETSANDTRANSFERS/Resources/Smart-National-ID-cards-in-Pakistan.pdf

Breckenridge, K. (2005): The biometric State: the promise and Peril of Digital Government in the New South Africa, Journal of Southern African Studies, Volume 31, Number 2, June 2005

Centro de Investigación Periodística (CIPER) (2016): "Grave falla en la red del Minsal dejó expuesta información confidencial de pacientes". Available at: https://ciperchile.cl/2016/03/05/grave-falla-en-la-red-del-minsal-dejo-expuesta-informacion-confidencial-de-pacientes/

Consejo Nacional de Evaluación de la Política de Desarrollo Social (CONEVAL) (2018): Informe de Evaluación de la Política de Desarrollo Social 2018, Ciudad de México: CONEVAL, 2018

Devereux, S. and Vincent, K. (2010): Using Technology to deliver social protection: exploring opportunities and risks, Development on Practice, Volume 20, Number 3, May 2010

Fan, V. (2013): The Early Success of India's Health Insurance for the Poor, RSBY, Center for Global Development, June 2013. Available at: http://www.cgdev.org/sites/default/files/archive/doc/full_text/CGDEssays/3120468/early-success-indias-health-insurance-rsby.html

Gelb, A. and Clark, J. (2013): Identification for Development: The Biometrics Revolution, Center for Global Development, Working paper 315, January 2013

Gelb, Alan and Decker, Caroline (2011): Cash at your fingertips: Biometric Technology for Transfers in resource-Rich Countries, Center for Global development, Working paper 253, June 2011

Gellman, R. (2013): Privacy and Biometric ID Systems: An Approach Using Fair Information Practices for Developing Countries, CGD Policy Paper 28, August 2013, Washington DC: Center for Global. Development Available at http://www.cgdev.org/sites/default/files/privacy-and-biometric-ID-systems_0.pdf

Gobierno del Peru (2018): "Cada vez más usuarias del programa Juntos reciben tarjetas Multired y capacitación en educación financiera". Available at: http://www.midis.gob.pe/index.php/es/centro-de-

informacion/informacion/publicaciones-midis/1376-cada-vez-mas-usuarias-del-programa-juntos-reciben-tarjetas-multired-y-capacitacion-en-educacion-financiera [11 May 2018]

Gobierno del Peru (2018)"Programa Juntos controla en tiempo real la salud y educación de niños y gestantes en Piura". Available at http://andina.pe/agencia/noticia.aspx?id=355308 [11 May 2018].

Gobierno Peru (2011): "Nota de Prensa: El programa Juntos controla en tiempo real la salud y la educación de niños y gestantes en Piura", 25 April 2011. Available at https://andina.pe/agencia/noticia-programa-juntos-controla-tiempo-real-salud-y-educacion-ninos-y-gestantes-piura-355308.aspx

Harvey, P.; Haver, K.; Hoffmann, J. and Brenda, M. (2010): Delivering Money. Cash Transfer Mechanisms in Emergencies, Save the Children, London, 2010

Hosein, G. and Nyst, C. (2013): Aiding Surveillance, Privacy International, October 2013

Longman, T. (2001): Identity cards, ethnic self-perception and genocide in Rwanda, in Caplan J, Torpey J. (ed.), Documenting individual identity. The development of state practices in the modern world, Princeton University Press, 2001

Mayhew, S. (2018): "Malta considers CCTV with facial recognition to curb antisocial behaviour", 26th September 2018. Available at https://www.biometricupdate.com/201809/malta-considers-cctv-with-facial-recognition-to-curb-antisocial-behavior

Moore, B. (1997): Victims and survivors: the Nazi persecution of the Jews in the Netherlands 1940–1945, London, Arnold, 1997

Office of the United Nations High Commissioner for Human Rights (2014): The right to privacy in the digital age, UN Doc. A/HRC/27/37 of 30 June 2014

Ramanathan, U. (2014): "Biometrics Use for Social Protection Programmes in India Risk Violating Human Rights of the Poor", post of 2 May 2014. Available at: https://socialprotection-humanrights.org/expertcom/biometrics-use-for-social-protection-programmes-in-india-risk-violating-human-rights-of-the-poor/

Rebecca Holmes, Nicola Jones, Rosana Vargas and Fabio Veras (2010): Cash transfers and gendered risks and vulnerabilities: lessons from Latin America, Backgound Note, Overseas Development Institute, October 2010. Available at https://www.odi.org/sites/odi.org.uk/files/odi-assets/publications-opinion-files/6042.pdf

Peru, Registro Nacional de Identificación y Estado Civil: Plan Nacional Perú contra la Indocumentación 2011-2015, Lima, Peru, January, 2012

Sepúlveda, M. (2018): Is biometric technology in social protection programmes illegal or arbitrary? An analysis of privacy and data protection, International Labour Organization, Extension of Social Security Paper, No. 59, Geneva, 2018

Sepúlveda, M. and Nyst, C. (2012): A Human rights approach to social protection, Ministry for Foreign Affairs of Finland, "Elements for Discussion Series", Erweko Oy, 2012

Setel, P.W.; Macfarlane, S.B.; Szreter, S.; Mikkelsen, L.; Jha, P.; Stout, S. and AbouZahr, C. (2007): Who Counts? A scandal of invisibility: making everyone count by counting everyone, The Lancet, Vol. 370, November 2007

South African Social Security Agency (SASSA) (no-dated): "You & your new SASSA payment card". Available at: www.sassa.gov.za

South African Social Security Agency (SASSA) (2018): Annual Report 2017/2018, SASSA, Pretoria, 2018.

United Nations High Commissioner for Refugees (2019): Global Trends. Forced Displacement In 2018, UNHCR.

World Bank (2012): Social Safety Net Global Expert Team, Safety Net How to: Identification of beneficiaries. Available at: http://siteresources.worldbank.org/SAFETYNETSANDTRANSFERS/Resources/281945-1291746977764/3-ids.pdf

World Bank (2015): The State of Social Safety Nets 2015. Washington, DC: World Bank

World Health Organization (WHO). 2013. "Gabon gets everyone under one social health insurance roof", in *Bulletin of the World Health Organization* 2013. Available at: https://www.who.int/bulletin/volumes/91/5/13-020513/en/