ESS – EXTENSION OF SOCIAL SECURITY

Is biometric technology in social protection programmes illegal or arbitrary? An analysis of privacy and data protection

Magdalena Sepúlveda Carmona

ESS – Working Paper No. 59

Social Protection Department

INTERNATIONAL LABOUR OFFICE, GENEVA

ISSN 1020-9581 ; 1020-959X (web pdf)

The editor of the series is the Director of the Social Protection Department, ILO. For more information on the series, or to submit a paper, please contact:

Isabel Ortiz, Director Social Protection Department
International Labour Organization
4 Route des Morillons
CH-1211 Geneva 22 Switzerland
Tel. +41.22.799.6226 • Fax:+41.22.799.79.62

Printed in Switzerland

Contents

Figures

Boxes

Acknowledgments

The author wishes to thank Isabel Ortiz, Karuna Pal, Christina Behrendt, Maya Stern-Plaza, Thibault van Langenhove and Leslie Bruguière for their comments and contributions to earlier drafts of this paper.

Executive summary

Social protection programmes require processing significant data amounts, including often-sensitive information such as household assets, health status and physical or intellectual disabilities. Increasingly, social protection programmes use unique, intimate biometric-technology data such as fingerprints, iris structure and face topologies. Inextricably linked to the individual body, they are more sensitive than other types of personal information.

Alongside use of information-technology and reliance on large databases as well as complex management information systems (MISs), the personal data social protection programmes collect can be easily shared, domestically and internationally, with a variety of public and private actors. While collecting and sharing personal information can increase efficiency in social protection programme management and monitoring, they can also threaten the rights, freedoms and personal security of those whose data is processed (applicants and beneficiaries) and indeed, of society at large.

Rights to privacy and data protection are well recognised in domestic and international law. Numerous legal instruments impose obligations on States regarding the protections of those rights. Social protection programme beneficiaries do not renounce their rights to privacy and data security when they provide their personal information. Social protection authorities must ensure all programmes comply with specific national and international rules that protect privacy and govern how information is processed.

A casual consideration of recent media reports, however, suggests breaches often occur. In Chile, for example, millions of patients' medical records – including those of HIV patients and women who had been sexually abused – were publicly exposed for almost a year. In the United States, politicians stigmatized welfare recipients based on digital records connected to Automated Teller Machine (ATM) cards used to collect benefits. In South Africa, private companies used millions of social protection beneficiary information to increase corporate profits to the detriment of beneficiary interests.

Additional examples have recently abounded. Technology's rapidly expanding power and reach enable a range of new threats to social protection applicants and beneficiaries' privacy, including unauthorised data sharing, covert surveillance and social control on programme beneficiaries. Mass information collection also encourages cybercriminals and hackers to undertake sophisticated scams. Emerging trends in counter-terrorism are putting pressure on government authorities to share the information they collect through social protection programmes with local, regional and international law-enforcement agencies.

Now more than ever, it is critical to address issues of privacy and data security in social protection programme design, implementation and evaluation. Yet in practice, this is rare. Social protection policymakers and practitioners currently tend to pay little or no attention to privacy and data security in relation to their programmes. In most countries, there are legal frameworks that govern privacy and personal data protection. Therefore, domestic law as well as international norms compel social protection practitioners to safeguard beneficiaries' related programme privacy, and data; these practitioners must prioritize policy options that do not undermine rights. This, too, is rarely seen in reality. Social protection programmes are often implemented without mechanisms that protect neither the rights of the individuals whose information is being collected nor the data itself.

The present paper seeks to guide social protection practitioners as they respond to critical questions for programme design and implementation, such as: what data should be collected? How do we ensure data will be lawfully processed? What data should or should

not be shared, and with whom? What data should be retained? For how long and in what manner? Who is responsible for the data a programme processes? What are data subjects' rights?

The paper focuses on non-contributory social protection programmes, particularly those that use biometric technologies. This focus is particularly relevant when private companies and donor agencies pressure programmes to use biometric technology. Technology use increases the risks beneficiaries as well as society face and underlines the importance of adopting explicit programme regulations to prevent, protect and redress potential breaches.

This work seeks to fill a gap in the literature and generate necessary debate on critical questions related to social protection programme information processing from a privacy and data perspective.

JEL Classification: I3, K38,

Keywords: social protection, social security systems, biometric-technology, data collection, data protection, right to privacy, management information systems

Abbreviations

ATM	Automated Teller Machine (ATM)
BISP	Benazir Income Support Programme (Pakistan)
CCT	Conditional Cash Transfer Programmes
CPS	Cash Paymaster Services Limited
CRS	Catholic Relief Services
EBT	Electronic benefit transfer cards (EBTs)
ECHR	European Court of Human Rights
GDPR	General Data Protection Regulation (European Parliament)
HSNP	Hunger Safety Net Programme (Kenya)
ILO	International Labour Office/Organization
MIS	Management information system
NADRA	National Database and Registration Authority (Pakistan)
OECD	Organization for Economic Cooperation and Development
OHCHR	Office of the United Nations High Commissioner for Human Rights
POS	Point-of-sale
SASSA	South African Social Security Agency
SMS	Short Message Service system
TANF	Temporary Assistance to Needy Families (United States)
UEPS	Universal Electronic Payment System
UIDAI	Unique Identification Authority (India)
UNHCR	Office of the United Nations High Commissioner for Refugees
WFP	World Food Programme

Introduction

Throughout their implementation stages, social protection programmes process considerable amounts of information collected from individuals and households. For example, during registration, a wide range of applicant information – name, age and income – is collected. The more complex the eligibility rules, the greater the demand for information and the greater the data protection challenges. Conferring benefits requires additional information to be collected and stored, such as health records, delivery locations, bank account and mobile phone numbers, or names of representatives allowed to collect payments on beneficiaries' behalf. The personal information processed under these programmes can be quite sensitive, e.g. household assets, health status or biometric data. The information is often stored in complex, integrated databases as well as elaborate management information systems (MISs), yet with few privacy and data security safeguards. In most cases, data subjects have little or no information about what data is collected, how it is used or for how long it will be retained. Moreover, the rapid advancements in technology facilitate information-sharing across international borders and between institutions. Biometric databases activate links between health records, border controls, retail, finance and banking information.

Despite the vast and sensitive nature of the data social protection programmes process, there is little information and scant political discussion regarding impacts. Social protection practitioners often pay little attention to privacy and data protection when designing, implementing and evaluating their programmes. [1] Perceived indifference to risks posed by lack of privacy and data protection is worrisome, particularly as we witness increased biometric-data use in social protection programmes around the world. In India alone, the Aadhaar Programme has assembled a biometric database on 1.25 billion individuals.

Critical social protection programme design and implementation decisions relate to applicants and beneficiaries' personal data. What data should be collected? How do we ensure data will be lawfully processed? What data should or should not be shared, and with whom? What data should be retained? For how long and in what manner? Who is responsible for the data a programme processes? What are data subjects' rights?

The present paper seeks to fill gaps in the literature and generate necessary debate on critical questions related to information processing in social protection programmes from a privacy and data perspective. The ILO Social Protection Floors Recommendation, 2012 (No. 202) (hereafter: R202) highlights the importance of protecting privacy and data in social protection programmes. In line with R202, States commit to "[e]stablish a legal framework to secure and protect private individual information contained in their social security data systems" (paragraph 23). [2] To this end, it is essential to: (a) understand the specific risks to privacy and data protection within social protection programmes, and (b) be aware of domestic and international norms related to privacy and data protection.

Governments, social protection authorities and practitioners should be aware of these norms as well as how best to integrate them into social protection programmes. They are

[1] It is interesting to note, for example, that among "Inter-Agency Social Protection Assessment Tools" (ISPAs), the tool for identification (ISPA, 2016) mentions the importance of protecting privacy, data-sharing and security, through a legal framework, several times. That said, the document lends little attention to the issue, dedicating only one appendix (Appendix 1) to "General Principles for Privacy in Identification".

[2] For further information on this recommendation, see ILO, 2017a and Dijkhoff et al., 2017.

required to take all necessary measures to ensure that a specific programme's information-processing does not infringe beneficiaries' rights to privacy and data protection.

As explored here, the right to privacy is protected in several international human rights instruments widely ratified by States, such as the International Covenant on Civil and Political Rights and the Convention on the Rights of the Child (see Chapter 2). So-called "data protection principles" call for data protection as well. These principles derive from several sources, including the United Nations *Guidelines for the Regulation of Computerized Personal Data Files* (1990) and the Organization for Economic Cooperation and Development's (OECD) *Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data* (2013). The paper examines applying these norms and standards to non-contributory social protection programmes (Chapter 3). It is critical for social protection practitioners to better understand how these norms and principles operate within social protection systems. In most if not all countries, at least some of these principles have been translated into domestic legislation, particularly nationwide data protection legislation. In the great majority of cases, however, especially in developing countries, data protection laws and principles are not consistently applied in social protection systems. For the most part, social protection programmes have expanded without serious considerations for beneficiaries' privacy and data protection, even when general data protection legislation may have been enacted in that country.

The paper also examines risks associated with social protection programme personal data processing (Chapter 4). Governments, social protection authorities and practitioners should understand risks and harms when handling data, particularly when biometric technology is used. While this technology offers a wide range of possibilities, its rapidly expanding power and reach require preventive measures that address emerging threats to privacy and data security. Subsequently, the paper proposes a set of minimum requirements social protection programmes should put in place to ensure respect of privacy and data protection (Chapter 5). By way of conclusion, the paper calls on social protection practitioners to prevent and address potential social protection programme privacy and data protection damages (Chapter 6).

1. The focus: biometric technology in Social protection programmes

In recent years, biometric technologies have come to be a common presence in people's daily lives around the world. From national identity cards to banking systems and mobile devises, the use of this technology is becoming ubiquitous. Social protection programmes are no exception. While many donors push for the introduction of biometric technology (Gelb and Clark, 2013), there is little debate on the impacts of this technology's use in social protection programmes; nor has there been any systematic or comprehensive mapping of programmes that use this technology.

This paper seeks to encourage wider debate on the use of biometric technology in social protection by raising critical questions that governments, donors, multilateral development banks, other development partners and the private sector should address before implementing or expanding biometric technology use in social protection systems.

While it focuses on issues of privacy and data protection, it also makes evident that broader questions regarding biometric technology use in social protection systems need to be addressed. Is biometric technology use appropriate and proportional in social protection systems? Is it the most effective way to improve beneficiary identification? To what extent does it respond to the implementation challenges social protection practitioners face? Is its use cost-effective in social protection systems? Are cost estimates for the introduction of biometric technology based on a realistic assessment of full implementation costs? Is its use in social protection inclusive? What measures are required to ensure inclusiveness? Are countries implementing this technology at levels that are fully capable of protecting the security and integrity of the people living in their jurisdictions? Do countries have sufficient technical and human capacity to implement this technology in social protection? Do they have the necessary technical, organizational and institutional resources to prevent and mitigate risks? Do they enjoy sufficient leverage to negotiate the most favourable terms for their populations when major transnational companies are involved in these systems' implementation? Who really benefits from the use of this technology? Who pays its costs? Ideally, all these questions – and many more – should be publicly discussed and assessed before implementing biometric systems in social protection programs, and on a regular basis once they have been implemented.

1.1. What are biometrics and why would their collection raise concern, particularly with regard to privacy rights?

Biometry is etymologically defined as the measure of living things. Applied to humans, it is "anthropometry science that studies with mathematics (statistics and probability) the biological variations within a specific group". [3] Biometry encompasses all means intending to identify an individual based on "metrics" of one or several of its physical, psychological or behavioural characteristics. It could be fingerprints, iris structure, face topology, DNA or any behavioural characteristic (signature, keystroke dynamics, and so on).

Unlike other possible identifiers, biometrics are not provided by a third party, nor chosen by the individual. Biometrics are produced by the body itself and are an individual's personal characteristics. Legally, the human body is an integral part of the person and all

[3] *Dictionnaire médical* de l'Académie de médecine, 2016.

physical information naturally fits into the personal information field. [4] Consequently, biometrics are by nature private information.

In addition, captured biometrics may contain much more personal information than the intended personal-unique-identifier (fingerprints, for example). This additional information may be later revealed in an analysis of collected information. For instance:

– Iris scans and gait can reveal disabilities or disease;

– The iris can indicate drug- or other medicine use;

– Face- and voice-recognition may provide information on a person's emotional state; (synergology [5] is also used to determine if a subject is lying or is experiencing a state of excessive agitation);

– Fingerprints can reveal the practice of certain activities or manual labour;

– DNA contains an individual's genetic inheritance.

Furthermore, risks to privacy differ depending on whether data leave traces or not (e.g. if they can be found in everyday life). DNA, fingerprints, palm prints and facial topology are notable for the traces they leave, and run great risk of being misused. According to France's Data Protection Authority, [6] fingerprints are almost as dangerous as DNA traces because they are omnipresent. It is impossible for an individual to not leave traces after his/her passage (CNIL, 2001). The discovery of a single trace provides access, by deduction or database interconnections, to all personal data – and without the relevant person's consent.

From a human rights perspective, 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 questions social protection practitioners rarely discuss: under what circumstances is processing biometric data legal and desirable? When does this technology's use threaten beneficiaries' rights and freedom? Can biometric data be used in ways other than originally specified or anticipated? When do links between databases breach data protection standards? What technological and/or policy mechanisms would impede or prevent unauthorized linkages?

Domestic and international norms should guide practitioners as they respond to these questions. More broadly, they would limit social protection practitioners' discretion for this technology's use in social protection systems by determining: (a) when its use is legal or non-arbitrary; [7] (b) the rights of beneficiaries whose data, including biometric data, are processed; (c) the obligations of social protection authorities and other actors who process

[4] European Court of Human Rights (ECHR), *S. and Marper* v. *the United Kingdom*, 4 December 2008, paras 66-81.

[5] *Synergology* is a form of non-verbal communication whose study implies a method of specialized interpretation, i.e. an analysis of unconscious body movements.

[6] Commission nationale de l'informatique et des libertés (CNIL).

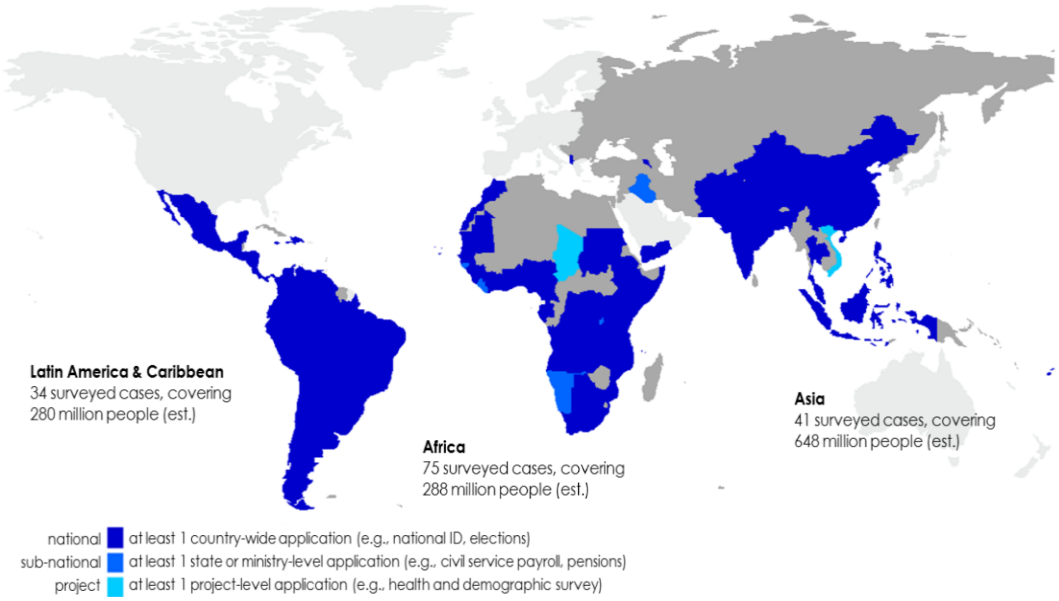
[7] As interpreted by human rights monitoring bodies, "arbitrary" goes beyond "unlawful" and features elements of disproportionate unreasonableness, injustice and unpredictability (Nowak, 2005). Thus, while the interference with privacy and data protection might be authorized by law, it should not be arbitrary.

and control the information; and (d) the mechanisms that should be put into place to safeguard that information. At a time when biometric technology use in social protection systems is expanding without comprehensive assessment of feasibility and costs, or independent research on impacts, understanding these legal standards is essential to securing the rights, freedoms and personal security of those impacted.

1.2. How often are biometric technologies used in social protection programmes?

Despite ongoing pressure to adopt biometric technologies, scant information is available regarding its various uses and global extent. In 2012, a survey on biometric technology use in developing countries showed that according to conservative estimates, over 1 billion people in those countries had had their biometrics taken (see figure 1); this number must be considerably higher at the time of writing this report (March 2018). In recent years, such technologies have become common for identification purposes in numerous cases ranging from airport security to banking transactions. Expansion of programmes such as Aadhaar, in India (see below), as well as biometrics' wide use for cash interventions during refugee crises (Lindskov Jacobsen, 2017) are particularly relevant to the present study.

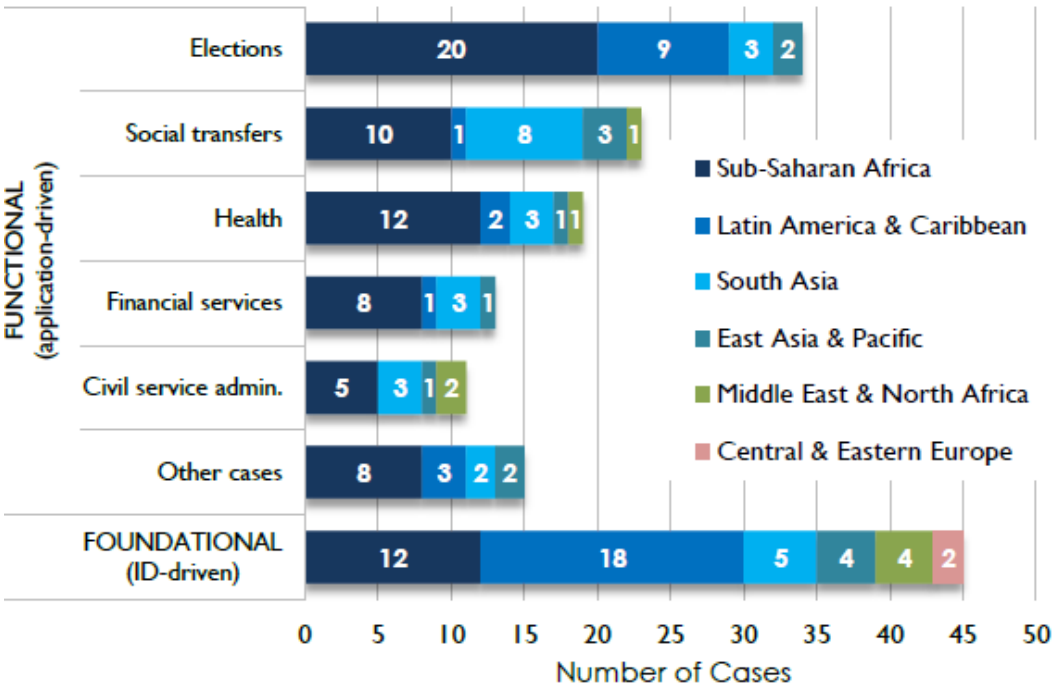
Figure 1. Biometric technology use in developing, low- and middle-income countries (2012)



Source: Gelb and Clark (2013).

The data shows the most common biometric technology use in developing countries is for national IDs, followed by voter IDs (see figure 2). This contrasts markedly with biometric technology use in developed countries, which focuses more on forensics and security. Very few developed countries use biometric technology in their national identity systems (Gelb and Clark, 2013, p. 2).

Figure 2. Representative developmental biometric cases (by type and region)



Source: Gelb and Clark (2013).

Donors lie behind many such initiatives. According to Gelb and Clark (2013), at least half the projects where biometric technologies have been implemented have been funded with official development assistance (Gelb and Clark, 2013, p. 20). In many cases, foreign companies provide these technologies (Gelb and Clark, 2013, p. 2).

While information on biometric technology use in social protection programmes is not systematically available, an examination of certain flagship, non-contributory programmes 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 programmes will continue and probably increase.

For example, beneficiaries of Kenya's *Hunger Safety Net Programme* (HSNP) receive a smart card with fingerprint information and an identifying photograph. Two sets of fingerprints can be stored on the card (for "primary" and "secondary" recipients). To claim benefits, programme recipients must go to pay-point agencies (small shops knows as *dukas*) and insert the smart card into a point-of-sale (POS) device that reads the card and scans the recipient's fingerprint, verifying the recipient's identity and authorizing the agent to hand over cash.

In South Africa, all social grant beneficiaries receive the *SASSA Debit MasterCard*. It captures biometric information such as beneficiaries' ten fingerprints, a voice recording and a photograph as well as their residential and mailing addresses and other contact information. To access the grant, beneficiaries must authenticate their fingerprints and voices using a

biometric reader. In 2013 there were reports of ten million *SASSA Debit MasterCards* active in South Africa. [8]

In Botswana, food-grant recipients receive a smart card called *SmartSwitch*. Operational since 2008, the card functions like a debit card into which monthly funds are deposited. The smart card contains beneficiaries' personal details and fingerprints. All card transactions require proof of beneficiaries' fingerprints. Some stores have card-swipe technologies that permit buying food at any time during the month. Merchants receive full payment, directly, in their bank accounts, within forty-eight hours of selling merchandise to cardholders. [9]

In Namibia, social protection beneficiaries receive a smart card called the *Epupa* card. A small team (specifically an Epupa paymaster and security officer) [10] visit designated pay-points in a truck (a so-called *bakkie*) with an ATM machine. Beneficiaries insert the *Epupa* card and present fingerprints for biometric identification to receive their cash. In Paraguay, some financial institutions in-charge of payments from the *Tekoporâ* cash-transfer programme have implemented a fingerprint-digitalization mechanism through which beneficiaries identify themselves and collect their transfers (Maldonado et al., 2011, p. 229).

In Benin and Nepal, a vaccination programme uses biometrics to eliminate redundant inoculations and prevent vaccine waste. The VaxTrac programme established a central database that compiles fingerprints of children receiving the vaccine as well as those of their mothers. VaxTrac also uses a Short Message Service system (SMS) to communicate with the parents and remind them of subsequent vaccination dates. [11]

Ghana is developing its National Household Registry (GNHR), a biometric-based social registry of all the nation's households. During the project's first phase (2016), biometric data from more than 138,000 households (comprising over 600,000 individuals) in Ghana's remote Upper West Region were added to registries. [12]

In Mexico, *Seguro Popular* is a healthcare initiative that provides benefits to the population's poorest segments and issues one biometric card to each beneficiary family. The

[8] MasterCard's Press Release: "Ten Million SASSA MasterCard Cards Issued to South African Social Grant Beneficiaries." Available at http://newsroom.mastercard.com/press-releases/ten-million-sassa-mastercard-cards-issued-to-south-african-social-grant/ [2 May 2018].

[9] Information gathered at the SmartSwitch Botswana website. Available at: http://www.smartswitch.co.bw/fcSuccess [2 May 2018].

[10] Epupa is the Namibian government's private payment-services provider.

[11] Information available at: https://healthmarketinnovations.org/program/vaxtrac [2 May 2018]. VaxTrac is a non-profit organization funded by the Bill and Melinda Gates Foundation. It deploys mobile, biometric-based vaccination registries for children under five in developing countries. Information available at https://www.gatesfoundation.org/How-We-Work/Quick-Links/Grants-Database/Grants/2010/ 11/OPP1025341 [2 May 2018].

[12] Information provided by GenKey, the company that supported the Ghanaian government's biometric-identification efforts. Available at: https://www.genkey.com/wp-content/uploads/2016/11/Social-Protection_ebook_EN-version-1.0.pdf [2 May 2018]. It is worth noting that GenKey's Chief Executive Officer, Michiel van der Veen (https://www.genkey.com/about-us/ [2 May 2018]), is also the founder of "Biometrics Africa," a resource platform that promotes biometric identification on that continent (https://biometricsafrica.com/ [2 May 2018]) and is the author of *Social protection: How biometrics makes a difference*" (Biometrics Africa, 2017). Available at: https://biometricsafrica.com/wp-content/uploads/2017/04/Social-Protection-how-biometrics-makes-a-difference-Biometrics-Africa.pdf [2 May 2018].

system captures all fingerprints of each member of the family above 10 years of age. [13] In 2013, 55.6 million people benefited from Seguro Popular. [14] Similarly, in Gabon, a health insurance for those living in poverty, known as GEF [15] and implemented by the *Caisse nationale d'assurance maladie et de garantie sociale* (CNAMGS), also uses biometric ID cards and serves 417,118 people as of 2011. [16] In both cases, fingerprints confirm the identity of the biometric ID card's bearer before he or she can access governmental services or healthcare. [17]

In some countries, such as Chile, Peru and Pakistan, national biometric IDs are compulsory for registering in social protection programmes. For example, to be eligible for benefits from Pakistan's *Benazir Income Support Programme* (BISP), women must register with the National Database and Registration Authority (NADRA) for biometric ID cards.

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). 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. [18] In addition to the general debate regarding the effectiveness of these conditionalities (Kidd, 2016), using biometrics to control class attendance is notably worrisome, in particular when it is carried out in the absence of appropriate legal frameworks that protect children's privacy and integrity. [19]

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 programmes. After a

[13] *Criterios específicos del sistema nominal en salud* (SINOS). Available at: http://www.seguropopularbc.gob.mx/net/downloads/Criterios-Sinos.pdf [2 May 2018].

[14] Source: World Bank Group. Available at: http://www.worldbank.org/en/results/2015/02/26/health-coverage-for-all-in-mexico [2 May 2018].

[15] GEF "Gabonais Economiquement Faibles" (Gabonese on low income).

[16] Source: WHO. Available at http://www.who.int/bulletin/volumes/91/5/13-020513/en/ [2 May 2018].

[17] https://www.gemalto.com/brochures-site/download-site/Documents/gabon.pdf [2 May 2018]. Note the biometric ID implementing company, Gemalto, serves both Mexico and Gabon. The organization has reportedly made more than 200 biometric deployments in eighty countries. See: https://www.gemalto.com/govt/biometrics [2 May 2018].

[18] See, for example, http://www.bn.com.pe/gobierno/programas-sociales/juntos.asp. See also press releases: "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] and "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].

[19] In the United Kingdom, for example, several guidelines protect children's data. See, for example, "Protection of Biometric Information of Children in Schools – Advice for Proprietors, Governing Bodies, Head Teachers, Principals and School Staff", Department of Education, March 2018. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/692116/Protection_of_Biometric_Information.pdf [2 May 2018]. For more information see https://www.gov.uk/government/publications/protection-of-biometric-information-of-children-in-schools [11 May 2018]. Guidelines of this type do not exist in developing countries.

free-of-charge enrolment process, beneficiaries receive a twelve-digit, randomly generated "Aadhaar number" that India's Unique Identification Authority (UIDAI) issues. [20] Aadhaar is the world's largest biometric database, covering over 90 percent of India's 1.25 billion inhabitants. [21] According to law, the programme was established "to provide for, as a good governance [sic], efficient, transparent, and targeted delivery of subsidies, benefits and service". [22] Since its establishment, the programme has been strongly criticised throughout India 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.

While using biometric technology for identification and/or authentication purposes in social protection programmes can offer some positive outcomes, such positives are hindered by a number of limitations. 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, p. 43). 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 OPM, 2014, p. 165).

Using biometric identifiers such as fingerprints and iris scans is also problematic for children. Fingerprints do not stabilize until around the age of fourteen; iris patterns stabilize at around 8 months but may be difficult to record in very young children (Gelb and Decker, 2011, p. 15). Other biometric technologies have presented problems. It has been reported that facial-recognition systems encounter difficulties when scanning darker-skinned individuals. Iris scans often do not adequately process scans from physically-impaired individuals or those with cataracts.

Garnering benefits when using biometrics will depend on the circumstances of the country concerned. A variety of factors, often not in place in low-income countries (reliable access to electricity and strong legal as well as institutional frameworks, etc.) are critical determinants of positive results. Economic and technical feasibility assessments must include rights- and dignity-related impact evaluations that could be critical to ensuring potential beneficiaries use the system as well as to minimizing overall negative impacts.

Unfortunately, comprehensive independent studies on biometric technology use in social protection programmes are not available; nor are there many accessible studies addressing risks to privacy and data protection.

This lack of attention to privacy and data protection in non-contributory social protection programs should not come as a surprise. These programmes aim to benefit most vulnerable members of society who hold additionally disadvantaged positions when it comes to making claims related to privacy and data security breaches. Entrenched stigma and anti-

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

[21] Anit Mukherjee: "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].

[22] "The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act", Act No. 18, 25 March 2016.

poor prejudices might prevent other, more privileged members of society from understanding risks.

Such stigmas may lead social protection practitioners to think non-contributory social protection programme beneficiaries are indifferent to whether a government security body, tax authority or private companies see personal data and how that information is used (McKee, 2012). A common perception assumes non-contributory programmes do not merit privacy and data security concerns. Those living in poverty should be grateful to receive a "benefit" in exchange for such information. For example, the Executive Director of the non-profit organization VaxTrac, [23] wondered why a mother should be concerned about her children being fingerprinted if they are going to receive a vaccine (LaMonica, 2014). These comments reflect indifference to sensitivities surrounding children's privacy and a lack of recognition that social protection as well as privacy are recognised children's rights (Articles 26 and 40, Convention on the Rights of the Child).

Privacy and data protection are not luxuries authorities or societies can deny to those living in poverty. Individuals entitled to social protection programmes have not renounced their rights to personal privacy and data protection in exchange for programme benefits. While it might be true that non-contributory programme beneficiaries do not often raise concerns about the way their data is processed, this is the outcome of stark power asymmetries between beneficiaries – often among society's most vulnerable and disadvantaged elements – and authorities that gather data and implement programmes.

That said, privacy and data protection concerns go beyond ensuring the enjoyment of equal rights among all people; they also have to do with social protection programmes' proper function. If privacy and data protection are not included in social protection programmes' design and management, expected programme objectives and outcomes may not be fully achieved. For example, possible public disclosure of personal information such as health conditions, disability or refugee status may deter potential beneficiaries from applying to programmes. At a time when four billion people worldwide have no access to social protection (ILO, 2017b), we cannot tolerate exclusions that arise from an unwillingness to address privacy and data protection issues.

[23] See note 12. More information about VaxTrac available at: https://healthmarketinnovations.org/program/vaxtrac [2 May 2018].

Box 1. Key terms clarified

Information processed within a social protection system can refer to:

Personal data, defined as any information relating to an identified or identifiable natural person ("data subject"). [1] This is information about a person whose identity is manifestly clear or can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his/her physical, physiological, mental, economic, cultural or social identity (EDPS, 2014). As noted, this is a broad concept covering much more than information that directly identifies an individual, such as a name, national registration number or taxpayer identification number. It can also include information that permits discovering the data subject's identity by means of further research, for example, via information related to remuneration, earned incomes and assets, government subsidies allocated to individuals, biometric information, IP addresses, traffic and location data, daily work- and rest-periods or corresponding breaks and intervals (EDPS, 2014). Consolidated statistical data, from which the data subject cannot be identified, is not deemed to be personal data.

Sensitive data refers to a special personal data category whose nature, when processed, may pose a risk to data subjects and indeed may require more stringent protective stipulations. [2] This refers, for example, to information that reveals personal characteristics such as racial or ethnic origin, health status, political opinions, religious or other beliefs, financial standing, sexual orientation, payment of welfare benefits, etc. International standards forbid gathering or processing sensitive information except under very specific circumstances. [3]

The rationale behind regulating particular data categories differently is an assumption that this data's misuse could have more severe consequences on an individual's fundamental rights – such as the right to privacy and non-discrimination – than would misusing other, "normal" personal data. [4] For example, misusing sensitive data such as health information or sexual orientation (if publicly revealed) may be irreversible and cause long-term consequences on individuals as well as their social environments.

Private and public bodies may process sensitive information only for specific purposes and under special conditions or exceptional circumstances. [5] These exceptions are usually set out at the domestic level and often correspond to those listed in the EU Data Protection Directive. [6] They include having data subjects' express consent to process sensitive information (but only for the purpose for which consent has been given); others' legitimate interests (but only in very specific situations) and substantial public interest (for which national law or a supervisory authority must provide).

A **data controller** is the individual (e.g. general practitioner) or the legal entity (e.g. government department) that controls and is responsible for safeguarding and handling personal information on computers or structured manual files. Data controllers have several legal responsibilities.

The **data processor** is the individual or legal entity that processes data on behalf of data controllers.

[1] See EU Data Protection Directive, Article 2(a) and Council of Europe (CoE) Convention No. 108, Article 2(a).

[2] See CoE Convention No. 108 (Article 6) and EU Data Protection Directive (Art. 8).

[3] See Article 8(1) of the EU Data Protection Directive and Article 6 CoE Convention No. 108.

[4] Article 29 Data Protection Working Party. 2011. *Advice paper on special categories of data ("sensitive data")*, 20 April 2011, Ref. Ares (2011) 444105. Available at:
http://ec.europa.eu/justice/article-29/documentation/other-document/files/2011/2011_04_20_letter_artwp_mme_le_bail_directive_9546ec_annex1_en.pdf [2 May 2018].

[5] Articles 8 (2) to (4) of EU Data Protection Directive provide specific exceptions to the prohibition of processing personal data. Under Art. 8 (2), sensitive data as defined in 8 (1) may be processed under the following conditions: (a) the data subject has given his explicit consent to the processing of that data; (b) the processing is necessary for the purposes of carrying out the obligations of the controller in the field of employment law; (c) the processing is necessary to protect the vital interests of the data subject or of another person; (d) the processing is carried out in the course of legitimate activities by a non-profit-seeking body with a political, philosophical, religious or trade-union aim; or (e) the processing relates to data which are manifestly made public by the data subject or are necessary for the establishment, exercise or defence of legal claims. Under Art. 8 (3), processing is allowed where it is "required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of healthcare services". Art. 8 (4) contains a catch-all provision allowing the processing of sensitive data for reasons other than those mentioned in Art. 8 (2) "for reasons of substantial public interest (...) either by national law or by decision of the supervisory authority". Art. 8 (5) is equally broad, stating the "processing of data relating to offences, criminal convictions or security measures may be carried out only under the control of official authority, or subject to derogations under national provisions providing suitable specific safeguards". The "Recitals of the Directive" (para. 34) mentions sample areas where there is a "substantial public interest": public health, scientific research, government statistics and social protection "especially in order to ensure the quality and cost-effectiveness of the procedures used for settling claims for benefits and services in the health insurance system". However, it is stressed that even in the case of these exceptions, authorities must provide specific and suitable safeguards so as to protect individuals' fundamental rights and privacy. Finally, in Art. 8(7), Member States may "determine the conditions under which a national identification number or any other identifier of general application may be processed". Processing national identification numbers or similar identifiers is not regarded as sensitive-data processing as understood in Art. 8 (1).

[6] See United Kingdom Data Protection (Processing of Sensitive Personal Data) Order 2000, No. 417, dated 17 February 2000, and the South African Protection of Personal Information Act, No. 4, 2013.

2. Privacy and data protection rights

Personal information (name, gender, address, fingerprints, household assets, health status) is processed at every step of a social protection programme's implementation. *Processing personal information* refers to any operation performed on that data, including its collection, registry, analysis, storage, transfer, consultation or use [24] (see figure 3).

Figure 3. Information Processing in Social protection programmes

Source: Author.

In social protection systems, information can be spoken (e.g. applicant interviews) or written (as on forms). It can be stored physically (paper files) or electronically, and the latter may include storage on a network or other digital storage (e.g. USBs, CDs or chip-cards). Information may be transmitted by many means, including by post, mobile phone or other digital network. Regardless of the way personal information is obtained or retained, it is protected by the privacy and data protection rights international and national standards enshrine.

Individuals do not waive their rights to privacy and data protection by becoming beneficiaries of social protection programmes. Beneficiaries of non-contributory programmes have rights related to their personal data that limit authorities' discretion regarding how government security bodies, tax authorities or private companies can access such data and how it is used. They have not renounced their rights to personal privacy and data protection in exchange for the benefits of the programmes in question.

[24] See Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (herewith referred to as CoE Convention No. 108), 1981, Art. 2(c); and Directive 95/46/ EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (herewith referred to as EU Data Protection Directive), Art. 2(b).

2.1. Content

Privacy and data protection are rights all should enjoy. [25] Both rights are expressions of principles of dignity, autonomy and all individuals' rights to develop their personalities and effectively participate in matters that impact them directly. These rights' common underlying objective is to prevent undue interference and grant individuals greater control over their own lives. As examined in this chapter, human rights treaties as well as many national legal frameworks enshrine these rights.

Today the right to privacy encompasses a wide range of areas such as persons' identities, names and genders, their honour, dignity or sexual orientation. The right to privacy extends to the home, family and correspondence (Sepúlveda et al., 2004, p. 249). The right to respect for one's private life includes the right to respect for one's personal information.

The right to data protection affords individuals' (data subjects') legal protection in instances where another person or institution (the data user) processes such persons' personal particulars (information).

Data protection limits authorities' ability to collect, publish, disclose or use others' information without their consent. Moreover, it requires authorities to establish mechanisms guaranteeing individuals have control over their personal information.

Rights to privacy and data protection are not absolute. They may be limited under specific conditions (e.g., for the exercise of other rights such as freedom of expression, national security or public health), [26] provided that interference is neither arbitrary nor unlawful. Their protection requires balancing choices, procedures and criteria to achieve a result that is legally and socially acceptable. Still, any limitations must comply with specific requirements that justify those interferences. Such requirements are contained in treaties protecting these rights, which provide, for example, that any interference must be allowable by law, must respect the essence of related rights, act in accordance with the principle of proportionality [27] and be necessary to protect others' rights and freedoms. [28]

Tensions may arise within social protection systems when balancing the right to privacy and data protection against requirements ensuring transparency and access to information, themselves critical safeguards against corruption, cronyism and waste (see box 2). In some jurisdictions, for example, bodies that oversee ensuring information access have decided transparency regarding beneficiary names and benefit amounts overrides privacy considerations (see box 3).

[25] It is well established that privacy and data protection are distinct rights. The right to data protection is related to, but nevertheless different from, a right to privacy. The right to privacy is broader than the right to data protection in that it often relates to home and family and covers many elements beyond personal information.

[26] See EU Data Protection Directive, Article 9.

[27] Human rights monitoring bodies, such as the European Court of Human Rights (ECHR) and the United Nations Human Rights Committee have further specified the nature of this principle. In general, it refers to whether the measure is reasonable in relation to the purposes sought. See for example ECHR, Case of *Leander* v. *Sweden*, Application No. 9248/81, 26 March 1987, para. 58.

[28] See for example Art. 52(1) of the EU Charter as well as the European Convention for the Protection of Human Rights and Fundamental Freedoms, Article 8(2).

Box 2. Ensuring transparency and access to information while guaranteeing privacy and personal information protections

In some cases, there can be trade-offs between transparency standards compliance and protecting social protection programme privacy and data. While sensitive data [1] social protection authorities hold should never be published or disclosed, a critical question is whether publishing recipients' names and their benefit amounts would breach privacy and data protection standards.

In many flagship, conditional cash-transfer programmes, all beneficiaries' names and amounts received by them are matters of public record. This is the case, for example, of Brazil's *Bolsa Familia*, *Prospera* in Mexico and *Seguridades y Oportunidades* in Chile. The argument for making this information available is a need to ensure transparency of use of public resources to help diminish fraud and corruption opportunities. In such cases, public interest overrides individuals' privacy. In Brazil, for example, the law establishes an obligation to publicly disclose beneficiaries' names and amounts received (Law 10.836, 9 January 2004, Art. 13). The disclosure appears in *Caixa Econômica Federal* as well as the federal transparency website (*Portal da Transparência*). [2]

However, in some social protection programme such as those for HIV and AIDS, breast cancer or domestic violence, or in programmes for persons with intellectual disabilities, more sensitive data come into play. Would it be legitimate to publish names of beneficiary from these programme categories? Would it entail an acceptable intrusion into their privacy? In these cases, a beneficiary list publication might be considered an intrusion into beneficiaries' right to privacy since it refers to sensitive data for which there are more stringent protections. And publication may also jeopardize individuals' safety or lead to their stigmatisation.

In some cases, technical solutions such as making certain aggregate and anonymized datasets and data visualizations available to the general public would avoid or decrease potential privacy vs. transparency trade-offs. In Indonesia, sixteen "sole registry" core indicators are available online in aggregate format (Barca and Chirchir, 2014, p. 41). In Costa Rica, citizens can only review non-identifying statistical data on its *Sistema de Información de la Población Objetivo* (Target Population Information System, SIPO) and its *Sistema de Atención de Beneficiarios* (Beneficiary Services System, SABEN) (Cecchini and Madariaga, 2011). Yet such technical solutions require careful assessment; aggregating information may still enable to draw precise conclusions about the private lives of those whose data is included in the registry. [3]

[1] See "Terminology", Box 1. [2] The Brazilian federal government established this transparency website to putatively allow all interested parties to monitor public money allocations. Accessible at http://transparencia.gov.br/ [2 May 2018]. [3] See Court of Justice of the European Union, ruling in joint cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and Others, ruling from 8 April 2014, paras. 26-27, 37.

Box 3. Enforcing rights to information access over privacy rights in Argentina and Chile

A 2014 Argentine Supreme Court ruling established that there is direct public interest in accessing social assistance programme beneficiary names. An NGO presented the case when denied access to information concerning 2006-2007 subsidy and social assistance beneficiaries. According to the court, ensuring access to information from such programmes ensures transparency and enables social accountability regarding how public officials allocate these subsidies. The court noted a request of this nature does not infringe rights to privacy, since it does not seek arbitrarily to gather beneficiary information. It also noted that ensuring access to this type of information is critical to guaranteeing social accountability regarding decisions the State may make as well as compliance with principles of rationality, effectiveness and efficiency. The court went on to assert that by providing access to such information, far from stigmatizing beneficiaries, the government helps ensure equity (Supreme Court of Argentina: Case 1172/03, 26 March 2014 ruling).

In Chile, the *Chile Solidario* (now *Seguridades y Oportunidades)* programme's legal framework expressly protects personal data of programme beneficiaries (Decree 235, 2004; and Law 19.949). As prescribed by law, the Ministry of Social Development can only share personal data of beneficiaries with public institutions that oversee programme evaluation. In such cases, individuals working at those institutions who have access to personal data must respect its confidentiality. The regulation also expressly declares tampering or unauthorized dissemination of personal data is by public officials is prohibited and will be legally sanctioned. Moreover, it notes any breach of obligatory confidentiality will be considered a serious transgression of the principle of administrative probity (Art. 22, Law 20.595, 17 May 2012).

In 2014 the Ministry of Social Development received a request for information related to all the social benefits and the respective amounts that a citizen had received in the past 7 years. The Ministry denied the request arguing the need to protect the citizen's right to privacy. The requester appealed the decision to the national Transparency Council (*Consejo para la Transparencia*).

The Transparency Council – an independent body established by law, to supervise compliance with the Chilean Access to Information Act – ordered the Ministry of Social Development to provide the information requested by the petitioners. The council argued that by receiving a benefit from the State, the scope of beneficiaries' right to privacy is reduced, in order to enable adequate social control of who is granted such benefits (*Transparency Council, Waldo Florit Otero* vs. *Ministerio de Desarrollo Social*, Case C1008-14, 23 September 2014).

2.2. National and international legal frameworks

Many national constitutions or bills-of-rights include a right to privacy. More than one hundred countries have adopted specific laws to ensure data protection and many have established specific monitoring mechanisms (e.g. national data protection authorities). [29]

International and regional human rights instruments protect these rights. At the United Nations, the right to privacy is enshrined in the Universal Declaration of Human Rights (Article 12), the International Covenant on Civil and Political Rights (Article 17), the Convention on the Rights of the Child (Article 16) and the International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families (Article 14). Most countries worldwide have voluntarily assumed the obligations these treaties include by becoming parties to them. In several jurisdictions (for instance in certain Latin American countries), obligations that international human rights treaties contain are assumed to take precedence over domestic law and in some cases over constitutional provisions. [30]

At the regional level, the right to privacy is contained in the American Convention on Human Rights (Article 11.2), the African Charter on the Rights and Welfare of the Child (Article 10), the African Union Principles on Freedom of Expression in Africa (Article 4), the European Convention for the Protection of Human Rights and Fundamental Freedoms (Article 8), the Charter of Fundamental Rights of the European Union (EU Charter, Articles 7 and 8), and the Arab Charter on Human Rights (Article 21). See table 1.

Moreover, there are specific instruments dealing with personal data protection, such as the United Nations Guidelines for the Regulation of Computerized Personal Data Files (1990), [31] the Organization for Economic Co-operation and Development's (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (2013), the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CoE Convention No. 108) (1985), [32] the Additional Protocol to CoE Convention No. 108 regarding Supervisory Authorities and Transborder Data Flows (1999) [33] and the European Parliament and Council Directive 95/46/EC on the Protection of

[29] See Dyson et al., 2014.

[30] See the Constitution of Chile (1980), Art. 5.2; the Constitution of Guatemala (1986), Art. 46; the Constitution of Nicaragua (1995), Art. 46; the Constitution of Brazil (1998), Art. 4; the Constitution of Colombia (1991), Art. 93; the Constitution of Argentina (1994), Art. 75; the Constitution of Ecuador (2008), Art. 11; the Constitution of the Bolivarian Republic of Venezuela (1999), Art. 2; the Constitution of Paraguay (1992), Art. 137; the Constitution of Costa Rica (2001), Art. 7; and the Constitution of El Salvador (2000), Art. 144.

[31] Adopted by General Assembly resolution 45/95, 14 December 1990.

[32] States parties to this convention are required to take necessary steps in domestic legislation to apply the principles it stipulates in order to ensure respect for all individuals' fundamental human rights when it comes to personal data processing. The Council of Europe Convention is potentially open to ratification by non-member states (Art. 23).

[33] Under this protocol, States parties are required to set up independent supervisory authorities to ensure the effective protection of human rights in personal data exchanges across national borders.

Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (1995) (i.e. EU Data Protection Directive). [34]

These data protection instruments have had a profound effect on the enactment of national legislation worldwide that regulates personal information collection, retention and use. In most countries, if not all, at least some of such principles have translated to domestic legislation, in particular national data protection legislation. According to a comprehensive global study, as of June 2017, 120 countries adopted Data-Privacy Laws. [35] Yet the level of detail of these laws, the existence of monitoring mechanisms and their enforcement is uneven. While data protection is strong in Europe, it is still incipient in other regions; in many developing countries the legal framework is inadequate and there are no appropriate judicial protections in cases of breach (Maqueo Ramírez et al., 2017). And even when legal frameworks protect privacy and data, this legislation is often not applied to social protection programmes or is not adapted to biometric data's particular character. The EU's General Data Protection Regulation, which becomes enforceable in May 2018 [36] (GDPR, see box 4) is an exception.

For the most part, social protection programmes have expanded in low and middle-income countries without serious considerations of beneficiaries' privacy and data protection, even when these should have been a critical concern under those countries' international human rights obligations or national data protection laws.

In some exceptional cases, protecting privacy and data has been included from constitutions – and all the way down in the legal hierarchy – within social assistance operational manuals. This is the case in Chile and Mexico. In Chile, the Ministry of Planning and Cooperation (*Ministerio de Planificación y Cooperación*) must legally guarantee *Chile Solidario*'s beneficiaries' privacy and data protection. [37] In Mexico, broad privacy and data protection in *Prospera*'s operational rules include obligatory compliance with federal laws

[34] This Directive was adopted in 1995. It has been translated by EU Member States into their respective national jurisdictions. A more stringent new "General Data Protection Regulation (GDPR)" was adopted in early 2016. On 4 May 2016, the official texts of the Regulation and the Directive were published in the EU official gazette. While regulation entered into effect on 24 May 2016, there is a two-year transition period. By 2018, Member States must transpose it to national law. The new General Data Protection Regulation strengthens citizens' rights. Individuals are to receive clear and understandable information when their personal data is processed. Whenever consent is required – and before a company can process personal data – such consent must be given by means of clear, affirmative action. The new rules will also strengthen individuals' right to expunging, meaning that should someone no longer want his/her personal data processed, and there is no legitimate reason for a company to keep it, it will be deleted (European Union: "How does the data protection reform strengthen citizens' rights?", Factsheet, January 2016. Available at: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=52404 [10 May 2018]).

[35] As of June 2017, 120 countries have adopted Data Privacy Laws, including Albania, Angola, Argentina, Bulgaria, Chile, Colombia, Costa Rica, Ghana, Mauritius, Mexico, Moldova, Morocco, Nepal, Nicaragua, Paraguay, Peru, the Philippines, Senegal, Tunisia, Vietnam and Zimbabwe. For the full list of countries, see Greenleaf, 2017.

[36] The GDPR will apply starting 25 May 2018.

[37] Decree No. 235 (2004), which regulates the application of Law No. 19.949 creating *Chile Solidario* establishes responsibility on the part of the Ministry of Planning and Cooperation (*Ministerio de Planificación y Cooperación*, MIDEPLAN) to guarantee protection of beneficiaries' privacy and data (Art. 7). Since October 2011, Mideplan has devolved to the Ministry of Social Development (*Ministerio de Desarrollo Social*).

protecting data and ensuring non-discriminatory information access. [38] However, a significant enforcement gap related to these regulations exists in both cases.

Box 4. 2016 EU General Data Protection Regulation (GDPR)

This 2016 European Union regulation is exceptional because it addresses the issue of biometric data. No such legislation can be found in other regional fora. The Regulation defines "**biometric data**" as "*personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data" (i.e. fingerprints)*.

Biometric data represents one of the categories defined as "**special categories of personal data**" and the regulation states processing it "**shall be prohibited**". Nonetheless, the language of the legislation foresees certain exceptions:

- If data subjects have given explicit consent to process their biometric data for one or more specific purposes.
- If biometric information processing is necessary to carry out the controller or data subjects' obligations and exercise their specific rights in matters related to employment as well as social security and social protection law.
- If processing is necessary to protect data subjects' vital interests and subjects are incapable of giving consent.
- If processing is necessary to establish, exercise or defend legal claims.
- If processing is necessary for reasons of public interest in public health.

The legislation's Article 9 expresses more specific exceptions. Additionally, it permits Member States to introduce other limitations on processing biometric information.

Considering that policy measures are only lawful if they comply with national and international legal frameworks, social protection authorities must ensure their programmes comply with specific national and international rules that protect privacy and govern information processing.

Privacy and data protection is not only critical to ensuring social protection programmes comply with applicable normative frameworks, but as well, to ensuring their effective functioning. A lack of privacy and personal data protection might undermine programmes' own objectives (e.g. protecting vulnerable populations), give rise to exclusion errors or expose beneficiaries to harm, stigmatization or discrimination. Human rights treaty monitoring bodies have already raised these concerns. For example, the Human Rights Committee – the International Covenant on Civil and Political Rights supervisory body – deemed that biometric identification (i.e. fingerprinting and retina scanning) of Canadian social assistance beneficiaries violated beneficiaries' right to privacy under the Covenant and should be eliminated. [39]

[38] Mexico's *Prospera* programme's operational rules (established by Official Decree, 30 December 2014). See Articles 9 and 12. Additionally the "Citizen's Manual on Social Programs" (*Manual Ciudadano sobre los Programas Sociales*) provides specific information on how the Federal Transparency and Access to Information Act applies to social protection programmes (*Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental*) Available at: https://www.tm.org.mx/wp-content/uploads/2012/08/1_pdfsam_Manual-Ciudadano-2001ssss.pdf [11 May 2018].

[39] Concluding Observations of the Human Rights Committee, Canada, UN Document CCPR/C/79/Add. 105, 7 April 1999, para. 16.

Table 1. Relevant provisions in International Human Rights Instruments

International Human Rights Treaties	Provisions
Universal Declaration of Human Rights (UDHR)	**Article 12:** No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.
International Covenant on Civil and Political Rights (ICCPR)	**Article 17:** (1) No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. (2) Everyone has the right to the protection of the law against such interference or attacks.
Convention on the Rights of the Child	**Article 16:** (1) No child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, or correspondence, nor to unlawful attacks on his or her honour and reputation. (2) The child has the right to the protection of the law against such interference or attacks.
Convention on the Protection of All Migrant Workers and Members of Their Families	**Article 14:** No migrant worker or member of his or her family shall be subjected to arbitrary or unlawful interference with his or her privacy, family, correspondence or other communications, or to unlawful attacks on his or her honour and reputation. Each migrant worker and member of his or her family shall have the right to the protection of the law against such interference or attacks.
Regional Human Rights Instruments	**Provisions**
American Convention on Human Rights (UDHR)	**Article 11:** (1) Everyone has the right to have his honour respected and his dignity recognized. (2) No one may be the object of arbitrary or abusive interference with his private life, his family, his home, or his correspondence, or of unlawful attacks on his honour or reputation. (3) Everyone has the right to the protection of the law against such interference or attacks.
European Convention for the Protection of Human Rights and Fundamental Freedoms	**Article 8:** (1) Everyone has the right to respect for his private and family life, his home and his correspondence. (2) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others. [1]
Charter of Fundamental Rights of the European Union	**Article 7:** Everyone has the right to respect for his or her private and family life, home and communications. **Article 8:** (1) Everyone has the right to the protection of personal data concerning him or her. (2) Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. (3) Compliance with these rules shall be subject to control by an independent authority.
Arab Charter on Human Rights	**Article 21:** (1) No one shall be subjected to arbitrary or unlawful interference with regard to his privacy, family, home or correspondence, nor to unlawful attacks on his honour or his reputation. (2) Everyone has the right to the protection of the law against such interference or attacks.
African Charter on the Rights and Welfare of the Child	**Article 10:** Protection of Privacy. No child shall be subject to arbitrary or unlawful interference with his privacy, family, home or correspondence, or to attacks upon his honour or reputation, provided that parents or legal guardians shall have the right to exercise reasonable supervision over the conduct of their children. The child has the right to the protection of the law against such interference or attacks.
African Union Principles on Freedom of Expression	**Principle IV:** Freedom of information. (1) Public bodies hold information not for themselves but as custodians of the public good and everyone has a right to access this information, subject only to clearly defined rules established by law.

[1] The European Court of Human Rights (ECHR) considers personal data protection fundamentally important to a person's enjoyment of his or her right to respect for private and family life (See Case of *S. and Marper* v. *the United Kingdom*, 4 December 2008, para. 103).

Source: Author's compilation.

3. General principles for privacy and data protection

ILO R202 sets out that States should establish a legal framework "to secure and protect private individual information contained in their social security data systems" (para. 23). This can be done by ensuring social protection laws, programme directives, operational manuals and/or policy guidelines incorporate so-called "information protection principles" included in the instruments that seek to protect the data mentioned above.

While in many countries these principles have been translated into national data protection laws (Greenleaf, 2016), they are not consistently applied in social protection systems. Even when countries have data protection laws in place, it would be highly desirable for social protection programme-related laws and regulations (e.g. social assistance law) to stipulate these information protection principles.

Box 5. Data Protection Principles

OECD Principles

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. The OECD guidelines have had a major influence on information protection legislation enactment and content in non-European jurisdictions, particularly Japan, Australia, New Zealand and Hong Kong. In North America, numerous companies and trade associations have formally endorsed the guidelines.

Specifically, the guidelines assert:

- **Collection Limitation Principle:** There should be limits to collecting personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
- **Data Quality Principle:** Personal data should be relevant to the purposes for which they are used and, to the extent necessary for those purposes, should be accurate, complete and up-to-date.
- **Purpose Specification Principle:** The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change-of-purpose.
- **Use Limitation Principle:** Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with [the Purpose Specification Principle] except: (a) with the consent of the data subject; or (b) by authority of law.
- **Security Safeguards Principle:** Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or data disclosure.
- **Openness Principle:** There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available for establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.
- **Individual Participation Principle:** An individual should have the right: (a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; (b) to have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him; (c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such a denial; and (d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.
- **Accountability Principle:** A data controller should be accountable for complying with measures that give effect to the principles stated above.

United Nations Guidelines for the Regulation of Computerized Personal Data Files

The United Nations Guidelines for the Regulation of Computerized Personal Data Files aim to encourage UN Member States to enact protection legislation based on the Guidelines. The Guidelines also aim to encourage intergovernmental organizations to process personal information in a responsible, fair and privacy-friendly manner. They contain the following principles:

1. *Principle of lawfulness and fairness.* Information about persons should not be collected or processed in unfair or unlawful ways, nor should it be used for ends contrary to the purposes and principles of the Charter of the United Nations.

2. *Principle of accuracy.* Persons responsible for the compilation of files, or those responsible for keeping them, are obliged to conduct regular checks on the accuracy and relevance of the data recorded and to ensure they are kept as complete as possible, to avoid errors of omission and

assure they are updated regularly or when information a file contains is used, for the duration of their processing.

3. *Principle of purpose-specification.* The purpose which a file is to serve and its utilization in terms of that purpose should be specified, legitimate and, when established, be made public or be brought to the attention of the person concerned. This to subsequently ensure: (a) all personal data collected and recorded remain relevant and adequate to specified purposes; (b) none of the said personal data is used or disclosed, except with the consent of the person concerned, for purposes incompatible with those specified; (c) the personal data's retention period does not exceed the time needed to achieve specified purposes.

4. *Principle of interested-person access.* Everyone who offers proof of identity has the right to know whether information concerning him is being processed and to obtain it in an intelligible form, without undue delay or expense, as well as to receive appropriate rectifications or erasures made in cases of unlawful, unnecessary or inaccurate entries and, when it is being communicated, to be informed of the addressees […].

5. *Principle of non-discrimination.* Subject to exceptional cases […] data likely to give rise to unlawful or arbitrary discrimination, including information on racial or ethnic origin, colour, sex life, political opinions, religious, philosophical and other beliefs as well as membership in associations or trade unions, should not be compiled.

6. *Power to make exceptions.* Departures from principles 1 to 4 may be authorized only if they are necessary to protect national security, public order, public health or morality, as well as, inter alia, the rights and freedoms of others, especially persons being persecuted (as in the case of the "humanitarian clause"), provided such departures are expressly specified in law or equivalent regulation promulgated in accordance with the internal legal system that expressly states their limits and sets forth appropriate safeguards. Exceptions to principle 5 relating to the prohibition of discrimination, in addition to being subject to the same safeguards as those prescribed for exceptions to principles 1 and 4, may be authorized only within the limits the International Bill of Human Rights and other relevant instruments legally prescribe in matters of human rights protection and discrimination prevention.

7. *Principle of security.* Appropriate measures should be taken to protect the files against both natural dangers, such as accidental loss or destruction, and human dangers, such as unauthorized access, fraudulent data misuse or computer-virus contamination.

The Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data
(CoE Convention No. 108)

The Convention's key principles are:

- **Data quality** (Art. 5)**.** Personal data undergoing automatic processing shall be: (a) obtained and processed fairly and lawfully; (b) stored for specified and legitimate purposes and not used in a way incompatible with those purposes; (c) adequate, relevant and not excessive in relation to the purposes for which they are stored; (d) accurate and, where necessary, kept up to date; (e) preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored.
- **Special categories of data** (Art. 6)**.** Personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, may not be processed automatically unless domestic law provides appropriate safeguards. The same shall apply to personal data relating to criminal convictions.
- **Data security** (Art. 7)**.** Appropriate security measures shall be taken for the protection of personal data stored in automated data files against accidental or unauthorized destruction or accidental loss as well as against unauthorized access, alteration or dissemination.
- **Additional Safeguards for the data subject** (Art. 8)**.** Any person shall be enabled: (a) to establish the existence of an automated personal data file, its main purposes, as well as the identity and habitual residence or principal place of business of the controller of the file; (b) to obtain at reasonable intervals and without excessive delay or expense confirmation of whether personal data relating to him are stored in the automated data file as well as communication to him of such data in an intelligible form; (c) to obtain, as the case may be, rectification or erasure of such data if these have been processed contrary to the provisions of domestic law giving effect to the basic principles set out in Articles 5 and 6 of this convention; (d) to have a remedy if a request for confirmation or, as the case may be, communication, rectification or erasure as referred to in paragraphs (b) and (c) of this article is not complied with.
- **Sanctions and remedies** (Art. 10)**.** Each Party undertakes to establish appropriate sanctions and remedies for violations of provisions of domestic law giving effect to the basic principles for data protection set out in this chapter.

The EU Data Protection Directive (Directive 95/46/EC)

The basic principles established by the EU Directive are:

- The obligation to collect data only for specified, explicit and legitimate purposes and to maintain that information only if it is relevant, accurate and up-to-date.
- The principle of fairness regarding the collection of data under which each individual is given the option of whether to provide the information requested or not, through a type of notice and opt-out procedure.
- Individuals must also be provided with an opportunity to learn the identity of organizations intending to process data about them and the main purpose for which that information is being collected or will be used.
- The EU Data Protection Directive also requires all data processing to have a proper legal basis and identifies the following legal grounds for the collection and use of data:
  - Contract;
  - Consent;

- Legal obligations;
- Vital interests of the data subject; and
- The balance between the legitimate interest of the people collecting or using the data and the people to whom the data relates.

- Data subjects' rights include:
  - the right of access to data;
  - the right to know where the data originated;
  - the right to have inaccurate data rectified;
  - the right of recourse in the event of unlawful data processing; and
  - the right to withhold data-use permission in certain circumstances.
- Where data is transferred from a European Union to a non-European Union country, the EU Data Protection Directive establishes a basic rule that non-EU countries receiving data must provide an "adequate level" of data protection.

The most relevant information protection principles for social protection systems include: [40]

- The collection limitation principle
- The fair and lawful processing principle
- Purpose-specification and use-limitation principles
- The security-safeguarding principle
- The openness principle
- The individual participation principle
- The accountability principle

These data protection principles establish the conditions under which information processing is legitimate. They also establish certain rights that data subjects hold. It is important to note that these principles overlap and are not strict categories. Moreover, each entails several rules.

The principles will be discussed with specific attention afforded to protecting personal information in non-contributory programmes that use biometric technology. A set of questions that can guide practitioners in assessing whether the corresponding principle is implemented in a given social protection programme follows each principle's analysis. These questions can also help social protection practitioners translate existing data protection laws into social protection regulations (e.g. social assistance laws or specific programmes' operational manuals).

These data protection principles imply several obligations for those in charge of social protection programmes as data "controllers" or "data processors" (see box 1). Those who implement social protection programmes should be able to demonstrate compliance with data protection principles at any time. These obligations imply corresponding rights for beneficiaries, such as the right to access their data at all times, have their data rectified if it is inaccurate and express objections if data processing leads to disproportionate results.

[40] These principles can be formulated in different ways, but the content of various versions remains the same.

3.1. The Collection Limitation Principle

There are limits to the collection of personal data. Some threats to privacy and personal data can be avoided by excluding certain information in the system or by establishing strict rules limiting data retention.

Unnecessary data collection not only implies risks to beneficiaries' rights but results in greater pressure to use data for purposes apart from those originally intended (ISPA, 2016, Annex A). While even apparently "safe" information may include major security and privacy dimensions, risks increase when sensitive data such as religious affiliations, race, ethnicity or linguistic origins are also collected. The data associated with each of these characteristics may be used for political purposes or to limit or remove rights.

In all phases of a social protection programme the information that is collected should be the minimum necessary to meet a clearly defined and articulated purpose (see "purpose-specification principle"). Moreover, to the extent necessary for those purposes, information storage should be accurate, complete and up-to-date. Data should be stored only as long as necessary.

Unfortunately, many programmes around the world collect excessive amounts of beneficiary information, much of which is of little use and is often inaccurate (Chirchir and Kidd, 2011, p. 7). Social protection programme designers should assess the amount of information to be collected, stored, shared and processed, and avoid the temptation to include information that "might be useful someday". Collecting minimal data amounts is critically important when programmes use biometric identification systems. Depending on intended uses, systems might function with just one or two biometric identifiers (e.g. fingerprints and iris scans).

For certain groups – such as those living in humanitarian crisis zones, asylum-seekers and refugees – even information that appears innocuous could be extremely sensitive due to those groups' special circumstances. In recent years, several initiatives have collected refugee biometric data, as, for example, Rohingya refugees in Bangladesh. They raise a number of concerns ranging from accusations of digital discrimination to creating unnecessary security risks should the data fall into the hands of persecutors in the country-of-origin (Rahman, 2017).

Box 6. The Indian National Rural Employment guarantee programme

India's *Mahatma Gandhi National Rural Employment Guarantee* programme (NREGA) collects a considerable amount of information as part of its registration process. Most information collected regarding individuals and households is personal and might even be considered sensitive, thus requiring stringent protection levels. It leads one to question whether the programme optimally adheres to the "collection limitation principle". The main question is whether the required information is appropriate, relevant, and not excessive in relation to programme objectives. Also, would it be possible to achieve programme objectives by processing fewer personal data?

The following are examples of information that must be provided when processing an MIS registry:

Household details, such as:

- Village name;
- Head-of-household name;
- Father/husband's name;
- Household minority-community affiliations, if any;
- Whether the household is a land-reform beneficiary;
- Whether the household enjoys "Small Farmer" or "Marginal Farmer" status;
- Whether beneficiaries are included under the Scheduled Tribes and Other Traditional Forest-Dwellers Act;
- Elector's photo-ID card number;
- Family ID from Household Survey BPL Census;
- Socioeconomic and caste census classification;
- Whether the household benefits from other social programmes such as Rastriya Swasthya Bima Yojana (RSBY) [1] and Aam Admi Bima Yojana. [2]

Individual details, including:

- Applicant name;
- Applicant individual photo;
- Applicant's bank/post office account number;
- AADHAAR number, if any;
- Mobile telephone number;
- Other applicant details, i.e. sex, age, disability status and relation to head-of-household.

[1] A Health Insurance Scheme for the Below Poverty Line families. [2] A Social Security Scheme for rural landless households.

Source: Government of India (2013).

Collecting minimum data not only helps protect beneficiaries' rights but also decreases the programmes' management information system costs. Each piece of information social protection programmes collect represents increased costs and makes MIS operations more expensive, complicated and stressful to the system (Chirchir and Kidd, 2011).

Limiting information collection is particularly relevant in countries with weak administrative capacities. An evaluation of Uganda's Social Assistance Grants for Empowerment (SAGE), has shown great difficulties in collecting and managing registration datasets even though collected data was relatively simple, such as age and household composition (OPM, 2013, p. 32). Problems collecting the information at registration could translate to inclusion and exclusion errors.

- Is collected data relevant and not excessive for a defined programme purpose? Are processed data categories necessary to achieve programme objectives?

- Could the same goal be achieved by reducing processed information amounts?

- Does the programme collect information only expected to be useful in the near future?
- Is the collected data accurate, complete, and up-to-date?

3.2. The Fair and Lawful Processing Principle

The primary principle of information protection laws is that personal information must be processed fairly and lawfully. [41] Thus, the personal data a social protection programme collects must be obtained and processed fairly (reasonably) and lawfully. Unless specifically permitted by law, there should be no secret or covert information processing.

It means social protection programme applicants and beneficiaries must give their free, informed and specific consent for their information to be processed. Consent may be given explicitly or implicitly (i.e. by acting in ways that leave no doubt the data subject agrees to his/her data being processed). However, sensitive-data processing requires explicit consent and must be unambiguous. [42] Generally, sensitive-data processing should be authorized by law. [43]

To determine data processing is fair, attention should also be paid to the method by which the information was obtained. Fairness implies a person is not unduly pressured into supplying information about him/herself to social protection authorities.

Informed consent is particularly important when collecting biometric data from beneficiaries. Informed consent means data subjects must understand all implications related to the information they provide: why the biometric information is being collected; who will have access to it; how it will be protected, stored, transmitted, and accessed; what the time limit for its use and storage is; when it will be deleted. Considering the vulnerability of data subjects in non-contributory social protection programmes, the information should be provided in an accessible (easy to understand) manner, including when data subjects may be illiterate.

Due to the sensibility of biometric information, social protection programmes should ensure no persons will be denied service or access to benefits because of their inability or unwillingness to provide biometric data or use a biometric system. An alternative should be offered where possible, and system design should include alternative processes for those unable to access the system.

The Fair and Lawful Processing Principle should be respected in all programme-implementation phases. For example, registration processes should be properly and carefully undertaken in order to not unreasonably intrude on individuals' privacy. Guarantees should be more stringent when the collected data is likely to give rise to discrimination, such as information on racial/ethnic origin or health status. This would be the case, for example, for programmes aimed at particularly vulnerable groups such as refugees or people with a specific health conditions (e.g. persons with disabilities or HIV and AIDS).

[41] See Art. 5 of CoE Convention No. 108.

[42] See CoE Convention No. 108; Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Art. 6; and EU Data Protection Directive, Art. 8(2).

[43] See Art. 7 of the EU Data Protection Directive. For exceptions, see Art. 8(2).

Fair and lawful information processing also means that information should be kept for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. [44] This means social protection programmes should establish a retention policy that clearly indicates time-limits for using and storing information as well as how it will be subsequently removed or deleted from databases. If data is no longer needed, social protection authorities should delete it or store it only in a form that does not permit data-subject identification (i.e. it should be made anonymous). This is particularly relevant for biometric information such as fingerprint data. The European Court of Human Rights has ruled a lack of safeguards to preserve and delete biometric data is a privacy rights violation. [45]

Box 7. Lack of privacy in registration offices

If registration office designs neglect privacy and confidentiality issues, applicants may be deterred from providing all necessary information – or even from registering for a programme. An evaluation of the South African Child Grant found that processing applications occurred in the presence of other applicants in severely overcrowded, shared offices or in open spaces where strangers looked on. Interviewees reported this affected people's freedom to speak openly.

Source: Goldblatt, Rosa and Hall, 2006.

- Do beneficiaries receive information on why information is being collected and how data will be used?
- How do beneficiaries express consent to share their personal information?
- Have beneficiaries given free, informed and specific consent to data processing? If not, is such processing necessary to carry out social protection authorities' obligations and exercise its specific rights? Is it authorized by national law and does that provide adequate safeguards?
- Are beneficiaries informed about who else will have access to the information? And how it will be protected, stored, transmitted and accessed?
- Has the personal information been collected in proper and careful ways in order to not unreasonably intrude on beneficiaries' privacy?
- Is a retention policy in place? Are beneficiaries informed about time limits on the use of stored information?
- Is personal information deleted as soon as data are no longer needed for programme objectives? If not, is the information retained in a non-identifiable form?

[44] See Art. 6(1)(e) of the EU Data Protection Directive and Art. 5(e) of CoE Convention No. 108.

[45] See ECHR case *M.K.* v. *France*, Application No. 19522/09, 18 April 2013.

3.3. Purpose specification and use limitation principles

Social protection programme applicants and beneficiaries should be informed about the programme's intended purpose, the reasons why data programme authorities have requested information and whether data will be shared with other government agencies. The purposes for which personal data are collected should be explicit, legitimate and specified at the time of data collection. [46] To that end, programme data collection forms may feature consent clauses and accessible information about the purpose of the data.

Personal data should not be disclosed, made available or otherwise used for purposes other than those specified at the time of data collection. Thus – as further explained below – using the data a social protection programme initially collected to combat terrorism or political dissent will constitute a new purpose and is, therefore, not authorized (except in the case of explicit consent or legislative approval). [47]

Personal data use for purposes not originally intended requires data-subject consent or legislative authorization. This means, for example, that fingerprints provided to enrol in social protection programmes should be used only to verify their bearers' identities within the programme, and that unauthorized persons will not examine fingerprint data.

To enhance efficiency across their entire social protection systems, many countries integrate social protection registries and establish MISs of varying complexity and sophistication (World Bank, 2015, pp. 36-37). In many countries, individual social protection programmes' MISs have been integrated into "single registries" (Chirchir and Farooq, 2016). In Kenya, for example, a single registry links MISs from five social protection programmes (specifically, the Old Age Grant, Disability Benefit, Orphans and Vulnerable Children's Cash Transfer, Hunger Safety Net programme and the World Food Programme's (WFP) Cash for Assets programme).

MIS integration often seeks to enhance programme efficiency and facilitate related monitoring. For example, data exchange between social protection programmes enables authorities to know all benefits a beneficiary receives and identifies inclusion errors or benefit duplications. Integrated information systems enable information traceability and provide efficient delivery-process management. As such, single registries act as "information warehouses" (Chirchir and Farooq, 2016). Single registries can subsequently be integrated within external databases such as income tax, civil registration or disability databases (see box 8).

[46] See EU Data Protection Directive.

[47] See for example, ECHR cases *Peck* v. *the United Kingdom,* Application No. 44647/98, 28 January 2003; *Perry v. the United Kingdom,* Application No. 63737/00, 17 July 2003; and *P.G. and J.H.* v. *the United Kingdom*, Application No. 44787/98, 25 September 2001; in which the European Court acknowledged that personal data cannot be used beyond normally foreseeable use.

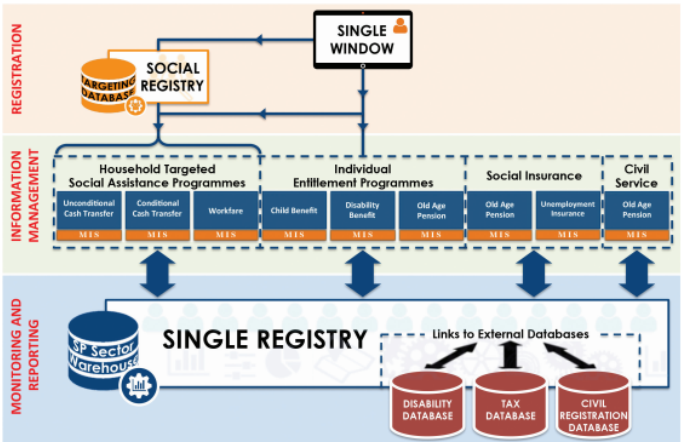
Box 8. Key terms, clarified: programme MIS, single registry and social registry

Chirchir and Farooq (2016) explain that there are three types of information management systems that can comprise the broader social protection related information management system:

Individual programme MISs (shown in the diagram's middle tier), divided by main social protection programme types found in developing countries: (1) household cash or in-kind transfer programmes targeted at those living in poverty, commonly known as "social assistance"; (2) lifecycle tax financed entitlement programmes for individuals (such as social pensions, disability benefits and child benefits); (3) social insurance programmes, such as old-age and disability pensions and unemployment insurance; and (4) pensions for public servants.

The ***single registry*** (shown in the diagram's lower blue tier) is an information "warehouse" corresponding to multiple social protection programmes and information nexuses between social protection programme MISs and other external databases that can be used during targeting and registration, such as income tax, civil registration and, if applicable, disability databases (as well as the social registry, if it exists).

The ***social registry*** is commonly known as a "unified targeting database". It provides information on households that can be used to select poverty-targeted social assistance programme beneficiaries. In effect, it ranks households from poorest to richest; poverty-targeted programmes use the ranking to target beneficiaries. They perform a much more limited function than single registries.



Source: Chirchir and Farooq (2016).

According to specification and use-limitation principles, integrating information between various databases should be expressly authorized by law that has been enacted prior to the occurrence. Such a law should prescribe: (a) what information should be disclosed; (b) to which agencies/programmes; (c) under what circumstances; and (d) the disclosure conditions (ISPA, 2016, Annex A).

In principle, only social protection authorities should access information collected for social protection purposes. Sharing that information with other national authorities or the private sector could infringe beneficiaries' rights to personal security, privacy and data protection and must be carefully assessed.

The "use-limitation principle" is critical in light of emerging counter-terrorism trends that pressure government authorities to share information between social protection databases and other public databases not related to social protection programmes (e.g. law enforcement databases). [48] The circumstances in which law enforcement officials may access social protection information, including any central database biometric data, require careful assessment.

[48] Some donors push for integrating "foundational" and "functional" registries with law enforcement registries both inside and between countries. See, for example World Bank, 2015.

Determining whether a privacy and data protection rights interference is reasonable (i.e. not arbitrary) requires balancing each case's circumstances precisely. For example, linking information about social protection beneficiaries to a tax payment database (as is the case in Argentina and South Africa) might be justified by an objective of improved targeting and fraud elimination. Similarly, "foundational" registry (i.e. identity registry) integration with "functional" registries (social protection systems, electoral authorities, etc.) may be permissible when legally allowed and proportional to specified purposes (e.g. improving various systems' efficiencies). However, integrating social protection databases with law enforcement registries (e.g. local, national, regional 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).

In sum, sharing social protection information (specifically, single registries or social registries) with other public or private databases should only occur when provided for by law, and should additionally be reasonable (proportional), strictly necessary and be ordered by well-established lines of accountability. The onus should fall to social protection authorities to demonstrate any database integration is legal, necessary and proportional to end-goals, as well as fully in line with the social protection programme/system's purposes. Avoiding doubts and clarifying uncertainties is essential to establishing written data protection and sharing protocols when integrating databases (see Chapter 5).

While these principles also apply to sharing or disclosing information with non-state agents such as private companies (e.g. payment-service providers and evaluating agencies), NGOs or independent consultants, some more stringent rules apply. According to the Inter-Agency Social Protection Assessments Partnership, other relevant factors for determining disclosure to non-state agents should be considered, including: (a) the proposed uses for, and the entity's lawful interests in, the information; (b) the benefits to the public and data subjects stemming from the user's handling the data; (c) the actual and potential risks to data subjects' rights, including their safety and privacy, arising from the user handling the data; and (d) the adequacy of the safeguards provided by or on behalf of the user (ISPA, 2016, Annex A, p. 43).

Moreover, data-sharing agreements with private actors should ensure: (1) strong privacy protections regarding the nature of the information disclosure; (2) clear regulation of purposes for which information may be disclosed and how that information may be used; and (3) a robust accreditation mechanism to govern access and use of such information (ISPA, 2016, Annex A, p. 43):

- Are the purposes for which personal data is collected explicit and legitimate?
- Are individuals informed about the intended purpose and reasons the information – including biometric data – has been requested? Is this information provided in an accessible (understandable) manner?
- Is collecting and storing beneficiaries' biometric information limited to those data strictly relevant to the purposes for which they are to be used?
- Is there any safeguard mechanism that ensures personal information provided under the programme, including biometric data, will not be used for purposes not originally intended without data-subject consent or legal authorization?
- If information sharing is explicitly authorized by law, do beneficiaries know what information may be shared, to which agencies and under what circumstances?

- Are there written data-sharing agreements (e.g. memoranda of understanding, contracts, or head-of-agency agreements)? Are these agreements known and publicly justified?

- Do data-sharing agreements comply with domestic legislation and international standards? Do they include details about who will share information and how it is to be shared? Are they regularly assessed?

- Is there any specific person within each organization responsible for agreement compliance? Is the agreement supported at all levels of the organization?

- Is there a system to eliminate or minimize the possibility of private actors taking advantage of collected data for unforeseen or for-profit purposes?

- Are there mechanisms to control private contractors?

- Are there clear mechanisms for monitoring and evaluating the implementation and impacts of data and information sharing initiatives?

3.4. The Security-Safeguarding Principle

Personal data should be protected during storage, transmission and use. This requires appropriate technical and organizational security safeguards against all risk types including loss, accidental or deliberate unauthorized data access, destruction, misuse, modification or unlawful disclosure. [49] Processing sensitive data, such as biometric data, requires higher security levels.

Information must be handled securely in all programme phases. For example, information provided at registration (including information from ineligible applicants) should be stored securely in an electronic database or paper filing system. At this stage, it is critical to note personal data should be stored in ways that enable reviewing eligibility decisions (and can hold decision-makers accountable); programmes should determine a retention policy (see "Fair and Lawful Processing Principle"). [50] Security mechanisms should be adapted to the technology programmes use. For example, programmes that use biometric-data smart cards or even just an ATM card should ensure cards cannot be forged, that third parties cannot access information stored on them and that the card can be blocked if stolen (ISPA, 2016, Annex A, p. 46).

Data security requires both the appropriate equipment (i.e. hardware and software) as well as necessary organizational guidelines. Organizational guidelines should include information for social protection personnel about data security rules, confidentiality obligations and obligations any existing data protection legislation stipulates; clear distribution data-processing responsibilities; and protecting access to programme installations, hardware and software. [51]

[49] See for example EU Data Protection Directive, Art. 17 (1), and CoE Convention No. 108, Art. 7.

[50] Databases can be designed to store background documents in the form of scans (Chirchir and Kidd, 2011, p. 6; Barrett and Kidd, 2015, p. 6).

[51] European Union Agency for Fundamental Rights, 2014, p. 91.

The Inter Agency Social Protection Assessments Partnership notes any database with personally identifiable information should feature policies and procedures to address breach notifications (i.e. notices to data subjects about personal data loss or unauthorized acquisition) as well as contingency plans that respond to actual data breaches.

This principle implies social protection authorities must undertake risk assessments of the appropriate security requirements. Considering how quickly technologies change, security requirements should be reassessed regularly:

- Do social protection authorities identify, evaluate, and prioritize security risks in each specific processing operation? Do they mitigate security risks as appropriate?
- Are there reasonable security safeguards against all risk types including personal data loss, unauthorized access, destruction, misuse, modification or disclosure? Is physical and digital infrastructure secure?
- What specific technical, institutional and physical security measures are in place to protect existing databases and MISs?
- Are social protection staff informed about their data protection obligations? How is compliance with such obligations implemented and monitored? Does staff with access to beneficiaries' information have access to any training or advice?
- Can staff access security training and education related to privacy and data protection?
- Are there policies that respond to breach notifications?
- Do social protection authorities regularly assess security risks?

Box 9. Management information system (MIS) security

Many social protection programmes use MISs to manage programme datasets and automate core business processes. [1] MISs enable information-flow and -management for key processes in social protection programmes; they typically feature five main components: application software, hardware, databases, telecommunications systems and staff (Chirchir and Kidd, 2011, p. 3). While MISs enable countries to more efficiently manage information and monitor it more effectively, strict security protocols should be in place to ensure data protection for each MIS component.

Social protection authorities are responsible for establishing measures for compliance with data protection rules in the context of their MIS processing operations. They should take all appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction, accidental loss, alteration, unauthorized disclosure or access, etc. Additionally, they should establish data-sharing protocols (see Purpose Specification and Use Limitation Principles). In some exceptional cases, the obligation to ensure MIS security is expressly established in programme operational manuals. For example, under Mexico's *Prospera* programme's operational rules, authorities are expressly required to take measures to ensure the security and integrity of the information the MIS contains, including by restricting database access. [2]

[1] For further information on MISs, see Barca and Chirchir, 2014. [2] Article 9, Official Decree, 30 December 2014.

3.5. The Openness Principle

In line with this principle, social protection programmes should be transparent in all practices and policies that relate to personal data. They should disclose, for example, the existence of a processing operation, what institution is responsible for that processing (i.e. the data controller) and what personal data are being processed.

This means, for example, that programme officials should directly provide applicants and beneficiaries basic information about their rights as well as data-processing operation

parameters. Information provided should enable beneficiaries to exercise their individual participation rights. [52]

A lack of transparency may lead to perceptions that programmes do not reach their rightful beneficiaries; mistrust regarding issues related to collecting, storing and processing personal information may decrease programme public support.

- Do beneficiaries know record-keeping systems, registers and databases that contain personal data exist?
- Do they know which personal data has been collected and stored?
- Is there a policy that ensures transparency about information collection and individual participation in that process?
- Do beneficiaries know the data's main purpose and uses?
- Do beneficiaries know who can access their data?

3.6. The Individual Participation Principle

Social protection programmes should ensure beneficiaries' access to and control of personal data, whether or not this information has been collected directly from them or from other sources.

All the applicant and beneficiary data that social protection programmes hold should be made available to applicants and beneficiaries upon request. Data subjects have a right to see and/or copy the data; a right to be given a reason if an access request is denied and a right to challenge that denial. [53] Social protection programmes should have simple, effective and accessible mechanisms through which beneficiaries can request access to the proprietary data social protection programmes' databases/MISs hold.

This is not only important to ensure personal data control, but also provides additional tools that check programme information accuracy. Knowing that beneficiaries can easily access information may prevent officials from falsifying it.

- Do beneficiaries have effective access to and control over their personal data storage within the programme? Are there sufficient guarantees that beneficiaries can exercise their rights to access and correction, as well as other relevant rights?
- Can beneficiaries request data corrections and deletions at any time?

[52] EU Data Protection Directive, Articles 10-11, further develop this principle.

[53] ISPA, 2016, Annex A, p. 47.

Box 10. Habeas *Data*

Constitutions of several Latin American countries – such as Argentina (Art. 43), Brazil (Art. 5), Colombia (Art. 15) and Paraguay (Art. 135) – offer protection of a key component in the right to information: the right to access information about oneself, whether held by public or private bodies and, where necessary, to update or correct that information. To protect these rights, these constitutions establish so-called *habeas* data. These are writs individuals submit to the courts to stop personal data abuses. In general, *habeas* data allow aggrieved parties to access personal information databases, edit and update data, ensure sensitive data remains confidential and remove sensitive personal data that could violate privacy rights.

Often, data protection laws further develop constitutional rights that protect personal data. This is the case, for example, in Colombia (Law 1.581, from 17 October 2012 and Law 1,266 from 31 December 2008), Argentina (Law 25,326, from 4 October 2000) and Paraguay (Law 1,682 from 16 January 2001). Other countries support similar data protection laws, including Spain (Organic Law 15/1999, from 13 December 1999), South Africa (Protection of Personal Information Bill) and the United Kingdom (Data protection Act, 1998).

Given that social protection administrations collect and process significant amounts of applicant and beneficiary information, *habeas* data can be a useful writ of protection, in particular when beneficiaries seek access to edit or update personal information that is included in social protection databases.

3.7. The Accountability Principle

Irrespective of beneficiaries' rights to recur to national data protection agencies (where available), social protection programmes should establish mechanisms beneficiaries can access when their privacy or data protection has been breached.

Social protection programmes should establish: (a) bodies to monitor programme-internal data protection compliance (which can include a programme Chief Privacy Officer); (b) a data-breach complaint protocol; (c) penalties in the event of data breaches; and (d) data-breach redress measures in the event of unauthorized access, use or disclosure.

Most developing countries do not support effective grievance and redress mechanisms for social protection programmes. Moreover, in exceptional cases, where a social grants appeals process exists, as with the South African Independent Tribunal for Social Assistance Appeals (ITSA), [54] or where there is access to a national human rights institution (ombudspersons, etc.) it is nonetheless unclear if such bodies would have sufficient technical and legal capacities to deal with beneficiary data protection issues.

- Is there an independent oversight body to monitor data protection compliance? Does it operate at the programme or national level (i.e. is it a national data protection authority)? Can the oversight body handle data-breach complaints? If so, does it comply with due-process guarantees?
- What happens in the event of a data breach (unauthorized access, misuse or disclosure of personal data, etc.)? Is there any clearly established procedure to follow?
- What sanctions will be imposed for data breaches?
- Do beneficiaries have access to effective remedies and redress when authorities violate their privacy and data? Are there effective mechanisms in place in case of fraudulent, misleading and unfair practices by private implementers?

[54] The ITSA is an independent tribunal of South Africa's Ministry of Social Development. It hears appeals related to the South African Social Security Agency (SASSA) rulings and was established by the Minister of Social Development in accordance with the Social Assistance Act regulation. For more information, see Art. 18 South Africa Social Assistance Act.

4. Risks associated with processing personal data in social protection programmes

This Chapter explores critical risks arising from lack of appropriate personal and sensitive data protection in social protection programmes. [55] Social protection practitioners often ignore these risks or leave them unexplored when designing, implementing and evaluating social protection programmes. Understanding existing privacy and data protection risks can help identify both legal and policy requirements that will ensure rights compliance.

Special attention must be paid to risks associated with privacy and data protection that arise from using biometric technology in social protection. As noted above, the past decade has seen increased use of biometric technologies in social protection programmes for beneficiary identification and authentication. Donors, multilateral development banks and development partners often encourage the use of these technologies. However, the danger of data abuse – especially in contexts without well-developed legal and institutional frameworks to protect rights, personal data, and privacy – is often not considered. [56]

The inclusion of biometric information will undeniably elicit interest in other sectors; it is likely at some point that police or other criminal investigators will request to use this information. [57] While some of the risks examined below are not specific to using biometric technology, its use might exacerbate them. Biometrics are unique to individuals and are therefore sensitive information that requires the highest protection levels.

Damage these risks might cause to social protection beneficiaries varies significantly (see box 11), ranging from stigmatization to exposure to bodily harm. Avoiding or minimizing damage depends on several factors, including establishing regulations and effective mechanisms that prevent government or third-party misuse or abuse as well as ensuring redress protocols in cases of breach. Minimizing risks also depends on infrastructure investments and qualified staff that can process data properly.

[55] While this study focuses on privacy and data protection, these are not the only risks raised by the use of biometric technology in social protection. Depending on specific national situations and programme objectives, using biometric identifiers poses additional risks related, for example, to both excluding vulnerable populations and personal security.

[56] ISPA, 2016, p. 17.

[57] Transparency reports from two private companies that collect DNA from customers for health and genealogy tests (23andMe and Ancestry.com) have reported interest in biometric databases by law enforcement agencies. See http://fusion.net/story/218726/23andme-transparency-report/ [6 May 2018].

Box 11. Overview: potential information damages, abuse or misuse that inclusion in social protection programmes may cause

If social protection authorities fail to establish appropriate data protection mechanisms or forego data security protocols, they expose beneficiaries and society at large to harm as classified below.

- Personal harm:
  - Bodily harm;
  - Loss of liberty, security and freedoms;
  - Economic damage due to the data's commercial misuse (for example, companies use data to exclude low-income people from credit).
- Intangible harm (which can be established objectively):
  - Discrimination or stigmatization
  - Embarrassment or anxiety to which publishing sensitive data gives rise (for example, disclosing beneficiary lists from breast cancer or HIV/AIDS programmes)
  - Unacceptable intrusion into private life
  - Reputational harm
  - Harm arising from exposure of identity, characteristics, activity, associations or opinions
- Societal harm
  - Political manipulation of the information
  - Excessive surveillance and control by authorities
  - Loss of social trust ("who knows what about whom?")
  - Selling information to private companies without proper controls that protect public interests

Source: Centre for Information Policy Leadership, 2014.

4.1. Arbitrary, Illegal or Unauthorized Data-Sharing

Recent years have seen increased interest in coordinating and harmonizing social protection programmes. To that end, countries seek to better integrate social protection data. In fact, information systems need to be organized for the various social protection programmes and benefits implemented by social protection systems. [58] However, sharing information included in social protection databases across various public or private databases not strictly related to social protection 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.

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. In Europe, for example, most countries' respect for privacy and data protection does not allow different databases to be integrated; these countries mandate using different identifiers for different domains (see box 12). In contrast, in developing countries where biometric identification efforts have recently been undertaken, donors and government authorities often encourage (or actively support) the

[58] See for example UNICEF, 2012.

widest possible integration of national identity databases, not only among public bodies but also in conjunction with private entities. [59]

Box 12. The risks of centralized storage of biometric data

Often large amounts of personal data are linked to a biometric ID and stored in a centralized database. This information may include names, date and place of birth, gender, fingerprints, eye colour, height, current address and photograph. It has been noted that in Europe whenever biometric data processing is permitted, centralized storage of personal biometric information is generally avoided.

Biometric data should be stored in encrypted form on a smart card or similar device. With this approach, use of biometric data for verification involves reading that data such that the biometric features can be compared with the data stored on the cards and/or devices through standard comparison procedures implemented directly on the cards and/or devices in question. Whenever possible, creating databases that include biometric information should be avoided.

If cards and/or devices are lost or mislaid, the risk that their biometric information may be misused is limited. To reduce the risk of identity theft, limited identification data related to the data subject should be stored on such devices. When biometric data "live" on a device that the data subjects physically control, specific encryption keys for reading devices should be used as an effective safeguard to protect against unauthorized access. Furthermore, such decentralized systems intentionally provide better data protection since data subjects stay in physical control of biometric data and no single point can be targeted or exploited.

Source: EU (2012).

Data-sharing between public databases

In developing countries, initiatives to integrate biometric identification efforts with other databases often fail to consider the significant privacy and security risks they involve (Hosein, 2011). Put bluntly, once biometric identification has taken place, multiple authorities will seek to use the information. In Nigeria, for example, an explicit objective of the national biometric ID was that it "be seen and used by road safety agencies as drivers' license; by the Electoral Commission as a voter's card; by the health authorities as health card; by the banks as a secure and genuine ID card, etc.". [60] In Malaysia, the compulsory national ID is a multi-purpose smart card called *MyKad*. In addition to proving identity and citizenship, *MyKad* can serve various other functions including as a driver's licence, health credential (the chip can contain basic health information such as blood type, allergies, organ implants, chronic diseases and information on beneficiaries or next-of-kin), an electronic wallet and an ATM card. [61]

While such measures might be considered purely a technical issue and an attempt to gain in efficiency and save on costs, the impact on people's rights must figure into the equation. An obvious such point is despite the existence of a common biometric card, the various agencies involved should not have access to the data of other agencies (for instance, bank authorities should not have access to user health information). Yet in examples like Nigeria, data protection is not always a priority (see box 13).

[59] See, for example, "Remarks by His Excellency, President Goodluck Ebele Jonathan, at the formal launch of the issuance process for the National Electronic Identity Card (E-Id Card)", held at State House, Abuja on Thursday, 28th August 2014. Available at: https://www.nimc.gov.ng/e-id-card-launch-speech/ [11 May 2018].

[60] Committee on Harmonisation of National Identity Cards. 2006. *Final Report of the Committee on Harmonisation of National Identity Cards*. Available at: https://www.nimc.gov.ng/docs/final_report.pdf [6 May 2018].

[61] Information acquired at the Official Web Portal of the National Registration Department of Malaysia, Ministry of Home Affairs. Available at: http://www.jpn.gov.my/en/informasi/aplikasi-utama/# [6 May 2018].

It is not uncommon for government agencies to share social protection data. That said, information-sharing does not always lead to positive results. For example, Los Angeles uses a "Coordinated Entry System" to match homeless individuals and families with appropriate available housing. [62] To ensure prioritizing its most vulnerable participants, the system uses an extensive survey called the VI-SPDAT ("Vulnerability Index-Service Prioritization and Decision Assistance Tool") that assigns "vulnerability scores". While final objectives are positive, problems arise because after gathering information, the system shares it with more than 168 separate state and federal organizations, including the Los Angeles Police Department. These organizations access the data free from oversight or any requirement to request warrants. As has been documented, sharing information on housing- and services-delivery to the homeless with other public databases may ultimately violate individuals' rights and bar society's most vulnerable from access to housing (Eubanks, 2018).

Box 13. Nigeria's national electronic identity card (e-card): are citizens' rights fully protected?

Established in 2007, Nigeria's National Identity Management Commission (NIMC) has issued a "general multi-purpose identity card" for all citizens and residents over sixteen. Programme enrolment involves recording the population's demographic and biographical data as well as a ten-fingerprint biometric capture, a facial image and cardholder digital signature. The card features MasterCard-branded prepaid functionality and twelve other applications. The objective is to issue over one hundred million e-Cards, implying the largest card rollout of its kind in Africa (NIMC, 2014).

While the national identity smart card project has been presented as a way to support financial inclusion, the system gives rise to important privacy consequences and provides the Nigerian government with a means of surveillance and social sorting (Lyon, 2007). The identification system enables Nigeria to collect vast amounts of personal data on citizens and residents alike which it subsequently shares across government agencies. In 2015, a vice-presidential directive ordered all government agencies collecting citizens' and legal residents' demographic and biometric data to aggregate all agencies' databases into a single databank whose information NIMC would warehouse and manage. [1] This data consolidation obviously increases the initiative's privacy and security risks yet concerns have thus far been ignored. Nigeria lacks adequate domestic legal frameworks for privacy and data protection. Were risks to materialize, it would nevertheless be too late to ensure the protection of those affected, particularly in cases of vulnerable individuals whose personal details were included in previous data harvests.

[1] National Identity Management Commission press release, "Data Collection Agencies Get Presidential Order to Aggregate Databases", 22 December 2015. Available at: http://www.nimc.gov.ng/press-release/ [8 May 2018].

Source: Information acquired at the NIMC website: http://www.nimc.gov.ng [8 May 2018] and https://www.biometricupdate.com/201305/nimc-and-mastercard-announce-nigerian-national-identity-smart-cards [11 May 2018].

Counter-terrorism measures

Emerging trends in counter-terrorism are highly problematic. Global terrorism threats exert pressure on national authorities to take stringent measures related to safeguarding national security. If such pressure leads to integrating social protection and law enforcement system databases – as some donors propose [63] – beneficiaries' privacy and data protection rights could be severely curtailed. Moreover, using social protection information for counter-terrorism measures could lead to distrust of the system and deter eligible participants from applying to much-needed programmes. Not least of all, it can give rise to a plethora of abuses while generating global problems (such as public health hazards). While there is little information regarding the use of social protection information in counter-terrorism efforts, related complexity and implications emerged from Osama Bin Laden's 2011 capture (box 14).

[62] https://www.lahsa.org/ces/ [8 May 2018].

[63] See, for example, World Bank, 2015.

Other potentially problematic measures include legislation that imposes more stringent rules on the financial sector; it might also have negative impacts on the rights of social protection beneficiaries. Pressure financial institutions feel to acquire more detailed knowledge on their customers (the "know your customer" rule, i.e. "KYC") may lead them to demand higher data-sharing levels when they provide social protection programme payment services. [64]

Box 14. A sabotage to public health in Pakistan

In 2011, the CIA organised a fake vaccination programme in the town where it believed Osama Bin Laden was hiding, part of an elaborate attempt to obtain DNA from the fugitive al-Qaeda leader's children (and compare it to samples from Bin Laden's sister, who died in Boston in 2010). One of the fake vaccine drive's immediate consequence was that legitimate vaccine workers along the Afghanistan-Pakistan border were physically threatened, accused of being spies; some were even killed. While Taliban commanders used the plot to ban polio vaccinations in parts of Pakistan, threats to health workers prompted the United Nations to withdraw vaccination teams from the region. Distrust of vaccination campaigns was also seen in countries such as Nigeria. By 2017, longer-term consequences surfaced: distrust of polio vaccination campaigns – the outcome of the CIA's fake scheme – ended up lowering Pakistan's vaccination rates.

Sources: *The Guardian:* "CIA Organised Fake Vaccination Drive to Get Osama Bin Laden's Family DNA", 11 July 2011. Available at: https://www.theguardian.com/world/2011/jul/11/cia-fake-vaccinations-osama-bin-ladens-dna [11 May 2018]. *Scientific American*: How the CIA's Fake Vaccination Campaign Endangers Us All, 1 May 2013 and *Vice*: "The CIA's Fake Vaccine Drive to Find Osama Bin Laden Lowered Vaccination Rates in Pakistan", 15 September 2017. Available at: https://tonic.vice.com/en_us/article/wjx559/fake-vaccine-drive-osama-bin-laden-lowered-vaccination-rates-in-pakistan [11 May 2018].

4.2. Data Disclosure or Unauthorized Third-Party Access

An act of disclosure arises when, contrary to the determination and will of the data subjects (including social protection programme applicants or beneficiaries'), parties with access to subjects' records reveal personal data to third parties.

Disclosing personal information of applicants or beneficiaries not only violates their privacy and data protection rights but could also expose them to discrimination, stigmatization, extortion or blackmail (see box 11). Even when some information held by social protection systems (including electronic databases) may be public (e.g. ID numbers), or available elsewhere, disclosures still run the risk of harm because, when combined, these discrete pieces of information provide a much more detailed picture of the person concerned. [65]

The fact that social protection programmes collect and use personal information, including biometric data, imposes an enormous responsibility on implementers, a responsibility they hold on behalf of both beneficiaries and society at large. Mass publication of private facts may harm not only beneficiaries whose information was revealed but also the society as a whole (for example, through a loss of social trust). Social protection authorities must take all necessary measures to secure personal data against risk of unauthorized access, particularly when processing highly intimate and sensitive data. To this end, adopting an adequate legal framework, specifically focused on social protection and

[64] E-course on "E-Transfers and Operationalizing Beneficiary Data Protection," Module 2: Legislation and Trends. Available at https://kayaconnect.org/course/info.php?id=516 [11 May 2018].

[65] When information relating to a person is collected, the total picture represented by the record of the facts is usually of such a nature that the person in question would like to restrict others from having knowledge thereof despite the fact that some of the information, when viewed in isolation, is not "private" or "personal".

containing appropriate safeguards to prevent personal data transmission or disclosure, should be considered a minimum requirement. [66]

Yet to avoid personal data disclosure, legal frameworks are not enough. From a human rights perspective, social protection implementers are obliged to adopt practical and effective measures to exclude any possibility of unauthorized access occurring in the first place. [67] 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.

Box 15. Chile: three million highly sensitivity health records disclosed

For more than fifteen years, Chile has supported a "Private-Life Protection Act" (Ley 19.628*, Sobre Protección de la Vida Privada,* 28 August 1999) that comprehensively enacts and develops data protection principles derived from international standards. The legislation includes specific sector regulations that ensure personal data protection.

The case of Chile's Ministry of Health is emblematic. In recent years, data protection has been a serious concern at a Ministry that has enacted a "General Policy on Information Security" [Resolution, RE 781, 14 October 2014] and more than forty resolutions and circulars regulating access, use and security regarding all the Ministry's internal electronic database computers, devices, programmes (software) and documentation. Additionally, the Ministry has established a "Sector Information Security Committee" (*Comité de Seguridad de la Información Sectorial*) whose task is to ensure the implementation of security control on the technology platform and to review and monitor both MIS security status and information security incidents.

When Chile's Ministry of Health implemented the sophisticated "E-Health" [*E-Salud*] preventive measures against information disclosure, data protection was high on the agenda. These measures also figured in the contractual obligations of ENTEL, the private company chosen to implement the system.

However, despite the establishment of this appropriate legal and institutional framework, from June 2015 to March 2016, more than three million medical records containing highly sensitive information such as names, IDs, addresses, case descriptions and prescription histories were publicly accessible to all 100,000 Ministry of Health employees, and even to the public at large. The breach concerned people undergoing HIV/AIDS treatments, women who had asked for the so-called "morning-after pill" following sexual assault and persons with mental disabilities, among others.

This sensitive information should have been encrypted and made available only to authorized officials, and such security measures should have been rigorously tested. Instead, all those files were easily accessible in the Ministry of Health computer network's so-called "shared folders", to all employees, free from any restriction. They were also easily accessible to external parties who had no sophisticated computer knowledge. This security breach caused serious harm to millions of people.

Moreover, when authorities learned of the public disclosure, neither established Health Ministry nor mechanisms the company providing the service-network had established were activated for ten months, until investigative journalists reported the case and moved the Minister of Health to take action. Had it not been for the efforts of those independent journalists, authorities would have likely delayed longer in reacting, harming victims even more.

While the Inter-American human rights system has yet to deal with the issue of data protection, the European Court of Human Rights has acknowledged the critical role confidentiality plays with respect to health data. The court declared crucial "not only to respect the sense of privacy of a patient but also to preserve his or her confidence in the medical profession and in health services in general. Without such protection, those in need of medical assistance may be deterred from revealing such information of a personal and intimate nature as may be necessary in order to receive appropriate treatment and, even from seeking such assistance, thereby endangering their own health and, in the case of communicable diseases, that of the community." [1]

[1] ECHR, case *Z. v Finland*, 25 February 1997.

Source: Information grab from Ministry of Health website. In particular, the press release entitled: "MINSAL instruye medidas para proteger acceso a sistema de información", from 5 March 2016, and the Centro de Investigación Periodística (CIPER)'s "Grave falla en la red del MINSAL dejó expuesta información confidencial de pacientes", from 5 March 2016.

[66] See for example ECHR cases: *I.* v. *Finland,* Application No. 20511/03, 17 July 2008 and *Z.* v. *Finland*, 25 February 1997, paras. 95-96.

[67] Ibid.

When social protection programmes outsource certain tasks (e.g. payment deliveries), information flows grow more complex, increasing privacy breach-related risks. The involvement of other agents (e.g. private stakeholders) requires putting in place additional security rules for data controllers (who determine the purposes for and means by which personal data are to be processed) and data processors (who process the data on behalf of the data controller). For example, when cash transfer programmes outsource payment delivery to specialized financial service providers (such as banks) or mobile phone operators (such as M-PESA in Kenya and MTN in Uganda) (Devereux and Vincent, 2010, p. 374), it is critical to establish a data- and information-sharing agreement between government and the private parties that clearly establishes who owns/controls the information and who holds responsibility for the databases.

The inherent complexities of CCT Programmes require processing of greater volumes of information. Information flows are more frequent and complex (specifically, information must be shared between schools, health services, social protection authorities and payment-service providers quickly and effectively to monitor conditionality compliance), entailing additional data- and privacy-protection challenges, particularly in countries with weak administrative capacities. Privacy breach and data protection risks increased for CCTs when appropriate safeguards were not in place.

4.3. Individual Covert Surveillance and Social Controls

Increasingly, States dispose of greater capabilities for conducting invasive, targeted and broad-scale population surveillance (OHCHR, 2014); additionally, society's most disadvantaged are often subjected to social control (ICHRP, 2010), particularly in cases of those receiving social assistance benefits. In the United States, for example, Temporary Assistance to Needy Families (TANF) beneficiaries are burdened with several restrictions when it comes to using electronic benefit transfer cards (EBTs) used to distribute benefits. While the EBT functions like any other debit card, in several states it cannot be used in certain locations (e.g. casinos or liquor stores) or to purchase certain products/services such as alcohol, cigarettes, tobacco and lottery tickets. [68] In 2014, federal and state agencies culled digital records of when and where some beneficiaries had withdrawn cash; politicians later used this information to stigmatize all recipients even though abuses were insignificant (Eubanks, 2018, p. 7).

Using integrated databases and biometric technology in social protection might further facilitate these types of intrusions. Biometric information can provide identifiers across systems and even across borders, tracking individuals in all contexts, allowing for information reuse and making sharing, linking and cross-checking information all faster (Hosein and Nyst, 2013, p. 30).

Rapid development in technology also raise concerns about specific risks of some biometric technologies as well as biometric data harvesting. Cumulative biometric information can be reused for a variety of purposes, unforeseen at collection time. For example, using digital photography in some programmes might pose risks related to facial-recognition technology, a particularly worrisome consideration in the context of governments' ability to curtail rights such as freedom of assembly and expression by identifying protesters. As noted above, fingerprint collection and storage in social protection programmes increases the risk that data will be used for purposes other than those for which the programmes provide, such as criminal investigations or indirect individual surveillance.

[68] http://www.ncsl.org/research/human-services/ebt-electronic-benefit-transfer-card-restrictions-for-public-assistance.aspx#table [8 May 2018].

Some social protection programmes legally prohibit the use of information for surveillance in order to prevent abuses and protect the rights of individuals. This is the case with India's Aadhaar programme, which expressly states that any attempt to track an individual using the Aadhaar number is an offence. [69]

4.4. Selling Data or Granting Private Companies privileged access

Social protection authorities and private companies (such as those in the global payment industry, e.g. MasterCard or Visa) frequently enter into commercial agreements. That said, some such agreements take place with no disclosure of the conditions of those agreements nor any establishment of clear rules and responsibilities regarding the personal data to which they afford access, nor do they establish redress mechanisms in information-abuse or -misuse cases.

The information and privileges companies gain in agreements with government authorities to roll out smart cards for social assistance programmes, or to accept those smart cards in their businesses, should be made public and subject to official oversight. These bilateral agreements may afford private companies privileged access to personal information of beneficiaries. Without adequate domestic regulatory frameworks and effective monitoring institutions, private enterprise could be let off the hook in cases of data misuse or may take advantage of social protection programme data for their own profits and in detriment to the interests of programme beneficiary or those of society at large.

States should establish appropriate legal and institutional frameworks to ensure social protection beneficiaries are protected against private-party abuses. Regulations should cover a broad spectrum of issues, from consumer protection to equal opportunity laws.

Recently, the case of abuse of social protection beneficiary information by private companies took the spotlight in South Africa. The South African Social Security Agency (SASSA) has a large biometric database and social grant recipients receive biometric smart cards – *SASSA Debit* MasterCards for which their fingerprints, photographs and even voices are captured. In 2013, ten million *SASSA Debit* MasterCards were reportedly active in South Africa. [70] Today the number should be considerably higher, since by late March 2017 there were 17.2 million grant beneficiaries. [71]

In 2012, SASSA hired Cash Paymaster Services Limited (CPS) to distribute social grant funds. Through its mother company, Net1 UEPS Technologies Inc. (Net1), CPS partnered with Grindrod Bank and MasterCard to exploit the biometric database and market financial services to SASSA beneficiaries. Although this practice contravenes the Protection of Personal Information Act, abuses have continued over the course of several years. In 2017, Black Sash, a non-profit organisation, submitted a motion to the Constitutional Court seeking to protect several SASSA beneficiary rights (*Black Sash Trust* v. *Minister of Social Development and Others*). Among other issues, the motion sought to protect beneficiaries' privacy and data protection rights. Consequently, the Constitutional Court ordered SASSA to include in its CPS contracts that personal data obtained in the payment process should remain private and was not to be used for any purpose other than grant payments. The order

[69] *The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act*, Act No. 18, 25 March 2016.

[70] MasterCard's Press Release: "Ten Million SASSA MasterCard Cards Issued to South African Social Grant Beneficiaries." Available at http://newsroom.mastercard.com/press-releases/ten-million-sassa-mastercard-cards-issued-to-south-african-social-grant/ [8 May 2018].

[71] SASSA, 2017.

even precluded inviting beneficiaries to "opt-in" to sharing confidential information for goods-and-services marketing. [72]

Data creep

Data creep refers to companies collecting data to assemble individual profiles. This profiling can be used against the interest of individuals, for example, by imposing high interest or credit costs or high insurance premiums when data identify high-risk consumers or consumers that can either or would pay more. For example, the *SASSA Debit* MasterCard can be used anywhere MasterCard is accepted, and beneficiaries may also use the card to purchase goods and airtime or pay utility bills. Those companies can then collect and sell the data that can then be used against the interests of individuals (see Breckenridge, 2005, p. 274).

Data vulnerability

In pursuit of profits from government contracts, private companies may have little interest or ability to provide optimal service or accommodate privacy-, security- and data protection demands.

Social protection programmes in several developing countries enable financial companies to create new markets and significant revenue sources. At a very minimum, the general public (including journalists and researchers) should be aware of these types of agreements; they should have access to all appropriate information (e.g. through access-to-information laws) upon request, as this is the sole way to guarantee effective oversight of those agreements. The legal and institutional framework should enable stakeholders to hold governments accountable for ensuring that public benefits always take precedence over private profits in agreements with private companies.

Proprietary rights

Property rights are another risk area related to the role of private corporate entities in social protection programmes, not strictly associated with personal data access but nonetheless critical to the efficient performance of programmes. Governments can get locked into proprietary systems with unfavourable conditions. Abuse risks are considerable since some such enterprises – that enjoy wide-ranging market control – may come to hold privileged positions. For example, one company, Net1 (former Aplitec, Applied Technology Holdings Limited), owns payment system intellectual property in South Africa, Namibia, Botswana and Swaziland. [73] When a single platform technology has a privileged position – which is currently the case in many developing countries – and since the most efficient technologies are usually in the hands of leading firms, there are risks of locking-in to proprietary systems where proprietors will undertake monopoly pricing or enter into bankruptcies that will cause systems to collapse, leaving recipients unpaid and unable to access their social transfers (Devereux and Vincent, 2010, p. 375).

[72] Constitutional Court of South Africa, *Black Sash Trust* v. *Minister of Social Development and Others (Freedom Under Law NPC Intervening)*, CCT 48/17, 15 June 2017.

[73] Information retrieved from official website. Available at: http://www.net1.com/about/corporate-history [8 May 2018].

Box 16. Learning privacy-protection from humanitarian practitioners

A lack of comprehensive discussion about privacy and data protection among *social protection* practitioners contrasts sharply with increasing attention *humanitarian* practitioners lend the issue, particularly in reference to protecting beneficiary data in programmes that use electronic transfers or e-transfers (CALP, 2013).

For example, to minimize potential private sector information use abuses, a number of humanitarian organizations that have implemented cash transfer programmes in response to the Syrian crisis in Lebanon and Jordan use pre-paid cards to reduce the personal information financial service providers undertaking payment delivery will require.

With pre-paid cards, there is no client relationship between the financial-services provider and the beneficiary. Instead, the aid agency has full control of the beneficiaries' financial information and their link to a particular card.

The office of the United Nations High Commissioner for Refugees (UNHCR) uses CSC Bank to deliver payments in Lebanon. UNHCR only provides the bank with beneficiaries' refugee registration case and phone numbers, not their names. The registration number links the debit card to each individual; only UNHCR links cards to particular persons. The contract with CSC Bank further states that personal information to which it has access must be kept confidential and secret. Similarly, Catholic Relief Services (CRS) opted to use Visa pre-paid cards (the VisaSwift Pre-paid); the organization only discloses card registration numbers as well as values to be transferred to the card company.

Source: E-course on "E-Transfers and Operationalizing Beneficiary Data protection", Module 4: Emerging Solutions. Available at: https://kayaconnect.org/course/info.php?id=516 [11 May 2018].

4.5. Cyberattacks

When information that social protection authorities collect is stored without establishing adequate security measures, a high risk of cyberattack exists. Additionally, factors like easy passwords, poor management, not updating software and untrained personnel make databases vulnerable to attacks and security breaches.

Increasingly, social protection data is stored in internet cloud services that private providers host; these may also be subject to attack. In those cases, agreements between governments and cloud services should include measures that not only prevent data breaches in the cloud but also establish minimum safeguards against hackers as well as sanctions and redress measures to address successful cyberattacks.

Despite considerable budget allocations for their prevention, cyberattacks are a major problem in developed as well as developing countries. Increasingly sophisticated attacks affect even the networks of developed countries where the underlying technologies are rapidly outdated. Cyberattacks on US government agencies, for example, have increased, prompting the White House to undertake massive new security efforts. [74] In 2015, the US Office of Personnel Management admitted that 5.6 million fingerprints were stolen from its database. [75] While noting that experts assert that the ability to misuse fingerprint data is limited, the agency acknowledges these odds could change over time as technology evolves. Once data is public, or falls into an imposter's hands, it can never again be private.

Additionally, the fact that once identifier indicators have been compromised, they cannot be reissued like signatures or passwords. This constitutes a major disadvantage of biometric technology. 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

[74] See "Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure", of 11 May 2017. Available at: https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/ [11 May 2018].

[75] Statement by OPM Press Secretary Sam Schumach on Background Investigations Incident published on its website, 23 September 2015. Available at: https://www.opm.gov/news/releases/2015/09/cyber-statement-923 [8 May 2018].

access the money or essential services upon which subsistence depends. While incentives for identity theft to defraud social protection programmes 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.

Social protection authorities must recognize risks and take measures to prevent being targeted for attack or breach. Collected information must always be treated as potentially valuable to others.

Box 17. *Aadhaar*: An alleged security breach

In early 2018, Indian newspaper *The Tribune* claimed its reporters were able to access Indian citizens' private information (names, e-mail addresses, phone numbers and post-codes) after gaining unrestricted access to the *Aadhaar* database. According to the newspaper, reporters entered the system by paying an anonymous seller and that individual was, in fact, connected to a group that accessed the database through former workers who initially processed *Aadhaar* cards. Reporters claimed that they were also offered software to print out individual identification cards. *Aadhaar* cards give access to various government services including fuel subsidies and free school meals.

While press reports triggered national debate, India's Unique Identification Authority denied any breach. That said, several actors have since raised concerns about system weaknesses in cases of identity theft. One major criticism is that *Aadhaar*'s design is based on a centralised database – the Central Identities Data Repository – where individual demographic and biometric information is stored. It has been argued that aggregating personal information in centralised databases makes that data vulnerable to exploitation as well as a target for hackers and identity thieves.

Sources: The Tribune. "Rs 500, 10 minutes, and you have access to billion Aadhaar details". Available at: http://www.tribuneindia.com/news/nation/rs-500-10-minutes-and-you-have-access-to-billion-aadhaar-details/523361.html, posted 4 January 2018 [9 May 2018].

Bhardwaj, Kritika: "Explainer: Aadhaar is vulnerable to identity theft because of its design and the way it is used". Wednesday, posted 2 April 201. Avalaible at: https://scroll.in/article/833230/explainer-aadhaar-is-vulnerable-to-identity-theft-because-of-its-design-and-the-way-it-is-used [9 May 2018].

Electronic Frontier Foundation. "Mandatory National IDs and Biometric Databases". Available at: https://www.eff.org/issues/national-ids [9 May 2018].

4.6. Data loss

When countries implement social protection programmes, a considerable amount of the investment goes to processing applicant and beneficiary information. Without adequate data protection – including the appropriate technical and organizational measures that secure it – risks arise that social protection authority data may be accidentally or unlawfully destroyed.

The unlawful destruction, accidental loss or modification of data due to faulty or careless collection, storage, or transmission may be extremely costly for social protection authorities. Such costs can be financial (e.g. data re-creation costs) but indeed can be political (e.g. a responsible minister's resignation) or even social (loss of trust in the system).

4.7. Political manipulation

If the personal data that social protection programmes gather is not properly protected, it can be subject to political manipulation in a number of ways. For example, abusive authorities may use beneficiaries' addresses or telephone numbers to deliver political propaganda to residences at election time.

Political manipulation risks increase when the system collects sensitive data such as religious affiliations or racial, ethnic or linguistic origins. Data associated with these characteristics may be used not only to limit or remove rights but also for political purposes. For example, influential ethnic groups may be disproportionately targeted for transfers at the same time dissenting ethnicities are systematically excluded (Devereux and Vincent, 2010, p. 374).

5. Minimum requirements for ensuring privacy and data protection in social protection programmes

Based on previous sections, the present chapter provides concrete recommendations for strengthening privacy and personal data protections within specific social protection programmes and social protection systems in general.

5.1. Develop privacy policies and specific operational guidelines for data protection

Even when countries have data protection laws, there must be specific regulations on data protection applicable to social protection systems that ensure social protection personnel are familiar with the provisions of the law and know how they should be implemented in the specific case of social protection programmes. Several measures could support this goal:

(a) **Develop sector-specific data protection policies.** Enacting data protection policy applicable to the entire social protection system would facilitate the implementation of consistent data protection legislation throughout a given country's social protection programmes.

(b) **Develop 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 alongside detailed guidelines that ensure all staff (and others who process personal data on behalf of the department) act in accordance with federal Data Protection Act principles.

(c) **Include data protection provisions in programme operational manuals.** This has been seen in flagship programmes like Chile Solidario [76] and Prospera. [77]

The objective should be to tailor the constitution or privacy and data protection laws' general provisions to the specificities of safeguarding social protection beneficiaries' privacy and data. Such specific regulations should seek to apply data protection principles within the social protection system (see Chapter 3).

Specific privacy and data protection regulations reaffirm the commitment of social protection authorities to protecting privacy rights in accordance with domestic legislation. Moreover, specific regulation facilitates the operational duties of staff while freeing them from a need to understand every complexity in general data protection laws or outcome of reform. Regulations should be widely disseminated among programme staff and should be supported by formal training.

The mere existence of specific regulations or policies may not provide adequate protection in the absence of proper oversight and enforcement. Therefore, the appointment of privacy and data protection committees or officers is advisable to ensure the implementation of data security controls, monitor MIS and IT security status and respond to information security incidents. These committees or officers should report directly to the highest authority within the programme or the social protection system.

[76] See footnote 37.

[77] See footnote 38.

Specific privacy and data protection regulations or policies should include:

- The type of information to be processed and the purpose for such information.
- How long the information will be retained.
- Who will be able to access the information, and how.
- How individuals access their proprietary information and how they can correct or update it.
- Complaints and enquiry systems that include avenues for redress.
- Expressly identifying authorities in charge of monitoring compliance.
- How regulations or policies will be promoted among staff; incentives as well as non-compliance sanctions.

5.2. Ensuring access to personal data

Social protection programme beneficiaries should have access to personal data the programme may hold, free from constraint, undue delay or expense. This includes information on processed data categories; the purpose for processing; who receives it; and the "logic" that underlies any automatic processing of personal information.

Information should be provided upon request regarding any decisions programme authorities make with reference to applicants or beneficiaries, in particular if such decisions limit or terminate benefit access. Such a consideration is key for applicants who have not successfully completed the enrolment process, enabling them to appeal exclusions.

Providing information access to beneficiaries is not only a right. It is, as well, a good mechanism for ensuring data accuracy, since beneficiaries can check their corresponding data entries. This right to access programme information is closely related to other rights such as the right to due process in administrative proceedings – including the right to be heard before decisions are taken – and the right to an effective remedy.

Individuals should be able to access their personal data:

- At any stage of the programme, free from discrimination.
- By an expeditious, economically accessible mechanism that enables them to correct or update their information as necessary.
- In an easily understood manner.

5.3. Implementing appropriate data security measures

Social protection authorities and private entities with access to social protection programme information should implement appropriate institutional, technical and physical measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access.

This requires social protection authorities identify, evaluate and prioritize security risks which may negatively impact beneficiaries. Assessments should be undertaken regularly when programmes adopt new technologies such as biometric identification.

Exemplary data security measures can include: [78]

- Developing secure physical and digital infrastructure.
- Securing premises and preventing unauthorized physical access to IT infrastructure.
- Securing connections and measures to define and protect logical security perimeters, such as firewalls, intrusion-prevention and -detection systems.
- Requesting IT system authorization and authentication procedures.
- Data encryption.
- Limiting access to specific, accredited staff; employee screening and clear enunciation of roles and responsibilities.
- Regular updates on data security rules to all social protection staff, alongside information on their obligations and ongoing data security training.
- Clear distribution of data-processing responsibilities.
- Implementing organizational measures to ensure appropriate reaction to security incidents, in particular personal data breaches.

5.4. Regulating data-sharing between government agencies

In some cases, sharing information among public databases can be positive. In Thailand, for example, the Universal Coverage Scheme's national beneficiary registry has been built based on the population database maintained by the Ministry of Interior. Healthcare providers use its national identification number to verify eligibility, track delivered services, settle claims and build shared medical records for each patient. Shared database system development and maintenance has reportedly improved efficiency and transparency related to managing the national social health protection system and has prevented public resource misuse (ILO, 2015).

To ensure positive results and minimize risks to privacy and data protection, social protection programme information sharing must be based on full transparency and must feature beneficiary consent and well-established lines of accountability. The onus should fall on social protection authorities to demonstrate that any linkage between public databases is legal, necessary and proportional to end goals, fully in line with programme/system purposes. Meaningful and proportional sanctions must be in place in case of any contravention. Sharing social protection data with law enforcement officials, intelligence bodies and other State organs whose duties are not directly linked to social protection programme purposes (for which the data was collected) should be expressly prohibited. Social protection programmes should not be used to profile or fingerprint those living in poverty.

[78] See EDPS, 2014.

At a minimum, the database links should be:

- Expressly authorised by law and further regulated by a Memorandum of Understanding between the two agencies. At a minimum, the law should prescribe what information should be disclosed; to which agencies/programmes; under what circumstances; the conditions for disclosure and lines of accountability.
- Strictly necessary and proportional to end goals, fully in line with programme/system purposes and not discriminatory.
- Transparent. Individuals should be informed about shared databases; affected individuals should consent to sharing information.
- Secure. Safeguards must ensure any sharing agreements (e.g. memoranda of understanding, contracts, or head-of-agency agreements) comply with domestic legislation and international standards.
- Accountable. Precise mechanisms should be in place to monitor and evaluate the implementation and impacts of data- and information-sharing initiatives.

5.5. Regulating private sector involvement

When the private sector is involved in social protection programme-related identification, registration or payments, it is important to establish strong privacy protections tailored to the nature of the information disclosed. A system of safeguards should prevent and sanction abuses or negligence regarding information shared. It should also eliminate or minimize the possibility that private actors take advantage of their access to collected programme data for unforeseen or lucrative ends and/or to the detriment of beneficiary interests or those of society at large.

Transparent, legally binding agreements that establish, *inter alia*, clear roles and responsibilities for parties; safeguards to prevent abuses; strict rules for database management and security; and specific mechanisms to control external contractors (e.g. surprise inspections) should regulate private sector involvement. Overall, programme beneficiary security, privacy and personal data should take precedence over private interests.

In line with the United Nations Guiding Principles on Business and Human Rights (OHCHR, 2011),[79] private companies should establish appropriate due diligence policies to identify, assess, prevent and mitigate any adverse impact on enjoyment of rights, including the right to privacy and personal data protection in connection with the business activities of the company. The Guiding Principles note that when enterprises have caused or contributed to negative human rights impacts, they have the responsibility to ensure remedies.

Contracts between social protection authorities and the private sector should enumerate:

- Benefits to the public as well as data subjects that stem from the company handling data.
- How the company will use information and how it will be managed between the company and the government.

[79] A/HRC/17/31, endorsed by the Human Rights Council in resolution 17/4, 16 June 2011. Available at: http://www.ohchr.org/documents/publications/GuidingprinciplesBusinesshr_en.pdf [9 May 2018].

- Who owns the data and what accreditation mechanisms will govern data access and use.
- Who is responsible for data processing related technical and procedural problems.
- Who monitors contract compliance.
- Who responds in case of abuses or negligence.
- Sanctions for breaches.

5.6. Establishing clear lines of accountability

Data protection authorities exist in some countries with data protection laws. When oversight bodies are in place, they should be afforded both mandates and resources to address social protection programme data protection issues.

Clear responsibilities and lines of accountability for privacy and data protection should be established as part of every social protection programme. One good practice is establishing specific oversight mechanisms within programmes (e.g. chief privacy officers) whose mandate is addressing data protection issues. Operational guidelines and staff manuals should also enumerate processes for reporting incidents, weaknesses and software malfunctions that may compromise privacy and data protection.

Ensuring accountability means guaranteeing transparency about how the data is collected, stored, used and potentially shared with other agencies/databases, as a fundament to raising concerns, making informed decisions or tendering complaints.

Checklist:

- At the national level, there is a well-resourced data protection authority with a mandate to address privacy and data security breaches in social protection programmes.
- At the sector level, there is an identifiable authority with final responsibility regarding privacy and data security.
- At the programme level, both an oversight mechanism (e.g. a chief privacy officer) and an express regulatory framework (i.e. operational guidelines and staff manuals) are in place.

5.7. Promoting continuous capacity-building and training for programme staff

Social protection programmes should ensure personnel can both perform technical tasks effectively (e.g. undertake data-capture, data-entry and system supervision) and also manage legal knowledge related to data- and privacy-protection. Because social protection practitioners often lack related skills, capacity-building in these areas is critical.

Staff training and awareness efforts should enable personnel to:

- Assess risks that arise from programme data collection.
- Develop better understandings of data protection principles and how they should be applied in social protection systems.

- Understand which remedies or improved practices can be activated to ensure privacy and data protection.

- Exercise managerial monitoring and supervision for privacy and data protection.

Many countries face additional challenges when ensuring necessary physical and technical support for protecting privacy and data. This may include, for example, access to adequate IT support services [80] for those working with MIS or access to adequate physical infrastructure to undertake beneficiary interviews.

[80] If the IT support is provided by an external company, social protection authorities remain responsible for ensuring data protection.

6. Final observations

Social protection programmes process considerable amounts of personal data. However, little attention is paid to how this data is processed (i.e. how it is collected, stored and transferred) in social protection systems. Insufficient attention to privacy and data protection constitutes a major oversight and becomes particularly problematic as these programmes increasingly take up the use of biometric technologies.

Biometric technology can potentially collect and aggregate vast amounts of information on individuals, including sensitive and detailed identity data. Biometric information use makes sharing, linking and cross-checking information faster and it can have both positive and negative consequences for individuals as well as for society at large. While it may help reduce fraud, it simultaneously gives rise to concerns that relate to the rights and freedoms of those whose data is processed.

The present paper identifies several risks associated with processing personal data, including biometric data, in social protection programmes. Domestic and international standards regulate information processing to prevent such risks. If social protection authorities do not comply with such standards, processing information could be illegal or arbitrary. The standards not only limit social protection decision-makers' discretion when designing and implementing programmes; they also enable decision-makers to identify the rights of those whose data has been processed as well as the obligations of data controllers and processors.

Considering that there is no common global standard for data protection, this paper stressed the need to adopt legal and institutional frameworks that safeguard privacy and data in social protection systems. That said, technologies evolve rapidly; legal and regulatory frameworks often lag behind. Thus, while adopting legal and regulatory frameworks to protect data and privacy are essential, they should be considered minimum standards; social protection authorities should strive to implement higher standards and guarantee regulatory frameworks receive regular reassessments.

When they protect privacy and data in social protection programmes, practitioners must ensure an adequate balance between protecting individual rights alongside public interests. These are not absolute rights and their protection requires balancing choices, procedures and criteria to achieve legally and socially acceptable outcomes.

Inadequate privacy and personal data protection in social protection programmes can have numerous negative impacts. First, it harms individuals via stigma, discrimination, abuses and exploitation. Second, it can undermine public support for programmes by diminishing public trust (as in cases of mass information disclosure). Third, it can compromise the effective functioning of social protection programmes' (e.g. inducing exclusion errors). Moreover, measures to adequately protect data, such as only collecting information relevant to programme purposes, may imply lower processing times and costs (e.g. less expensive MIS systems).

Social protection practitioners must no longer ignore the privacy and data protection issues that relate to their endeavours. As some donors, multilateral development banks and development partners push for the use of biometric technology, broader debate on the topic is essential. What risks are associated with the use of biometric technology? Is using biometric technology appropriate and proportional in social protection systems? Is it reliable and feasible in the national context? In what contexts should social protection programmes use biometrics? To what extent does the technology respond to the implementation challenges social protection programmes face? Is biometric technology use cost-effective in social protection systems? Who benefits from using these technologies? We can no longer neglect such pressing questions.

References

Barca, V.; Chirchir, R. 2014. *Single registries and integrated MISs: De-mystifying data and information management concepts*, Australian Government, Department of Foreign Affairs and Trade (Barton ACT, Australia, Commonwealth of Australia).

Barrett, S.; Kidd, S. 2015. *The design and management of cash transfer programmes: an overview*. KfW Development Bank, Materials on Development Financing No. 3 (Frankfurt am Main, KfW Group).

Breckenridge, K. 2005. "The biometric State: The promise and peril of digital government in the new South Africa", in *Journal of Southern African Studies*, Vol. 31, No. 2, pp. 267-282, DOI: 10.1080/03057070500109458.

CALP (Cash Learning Partnership). 2013. *Protecting Beneficiary Privacy: Principles and operational standards for the secure use of personal data in cash and e-transfer programs*. Available at: http://cashlearning.org/downloads/calp-beneficiary-privacy-web.pdf [1 May 2018].

Cecchini, S.; Madariaga, A. 2011. *Conditional cash transfer programmes: The recent experience in Latin America and the Caribbean*, Cuadernos de la CEPAL, No. 95 (Santiago, Chile, Economic Commission for Latin America and the Caribbean (ECLAC). United Nations publication).

Centre for Information Policy Leadership. 2014. *A Risk-based approach to privacy: Improving effectiveness in practice*. Available at: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/white_paper_1-a_risk_based_approach_to_privacy_improving_effectiveness_in_practice.pdf [1 May 2018].

Chirchir, R.; Farooq, S. 2016. *Single Registries and Social Registries: clarifying the terminological confusion*, Pathways' Perspectives on social policy in international development, Issue No. 23, November 2016 Kent, United Kingdom, Development Pathways). Available at: http://www.developmentpathways.co.uk/resources/wp-content/uploads/2016/11/Single-and-Social-Registries.pdf [1 May 2018].

—; Kidd, S. 2011. *Good practice in the development of management information systems for social protection.* Pension watch Briefings on social protection in older age. Briefing no.5 (HelpAge International, London).

CNIL (Commission Nationale de l'Informatique et des Libertés - French data protection authority). 2001. *21^{e} rapport d'activité 2000* (Paris).

Council of Europe. 1981. *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, European Treaty Series, No. 108 (Strasbourg).

—. *Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* (Strasbourg, 28 January 1981).

Devereux, S.; Vincent, K. 2010. Using Technology to deliver social protection: Exploring opportunities and risks, *Development in Practice*, Vol. 20, No. 3, 367-379, DOI: 10.1080/09614521003709940.

Dijkhoff, T.; Letlhokwa Mpedi, G. (eds.). 2017. *Recommendation on Social Protection Floors: Basic Principles for Innovative Solutions* (The Netherlands, Kluwer Law International B.V.).

DLA Piper. 2016. *Data protection Laws of the World Handbook*. Available at: https://www.dlapiperdataprotection.com/index.html [30 May 2016].

Dyson, A; Halpert, J; Ramos, D.; van Schaik, R.; Thiel, S.; Umhoefer, C. A. F.; Van Eecke, P. 2014. *Data Protection Laws of the World Handbook: Third Edition* (DLA Piper). Available at https://www.dlapiper.com/en/us/insights/publications/2014/01/data-protection-laws-of-the-world-handbook/ [10 May 2018].

EDPS (European Data Protection Supervisor). 2014. *Guidelines on data protection in EU financial services regulation* (Brussels). Available at: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Thematic%20Guidelines/14-11-25_Financial_Guidelines_EN.pdf [2 May 2018].

Eubanks, V. 2018. *Automating inequality: How high-tech tools profile, police, and punish the poor* (New York, St. Martin's Press).

European Parliament; Council of the European Union. 1995. *Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, 24 October 1995, Official Journal of the European Communities, No. L 281/31 (Luxembourg).

European Union. 2012. *Opinion 3/2012 on developments in biometric technologies*, adopted on 27th April 2012. Article 29 Data Protection Working Party, 00720/12/EN WP193 (Brussels, European Commission). Available at: https://www.apda.ad/system/files/wp193_en.pdf [1 May 2018].

European Union Agency for Fundamental Rights. 2014. *Handbook on European data protection law* (Luxembourg, Publications Office of the European Union).

Gelb, A.; Decker, C. 2011. *Cash at your fingertips: Biometric technology for transfers in resource-rich countries*, Center for Global Development, Working paper 253 (Washington, DC, Center for Global Development).

—; Clark, J. 2013. *Identification for development: The biometrics revolution*. Center for Global Development, Working paper 315 (Washington, DC, Center for Global Development).

Goldblatt, B.; Rosa, S.; Hall, K. 2006. *Implementation of the Child Support Grant*. Centre for Applied Legal Studies, University of the Witwatersrand and Children's Institute, University of Cape Town.

Government of India. 2013. *The National Rural Employment Guarantee Act 2005 (NREGA), Operational Guidelines, 2013, 4th edition* (New Delhi, Ministry of Rural Development).

Greenleaf, G. 2017. *Global Tables of Data Privacy Laws and Bills (5th Ed 2017)*, 145 Privacy Laws & Business International Report, 14-26. Available at SSRN: https://ssrn.com/abstract=2992986 [10 May 2018].

Harvey, P.; Haver, K.; Hoffmann, J.; Murphy, B. 2010. *Delivering money: Cash transfer mechanisms in emergencies* (London, The Save the Children Fund). Available at: http://www.actionagainsthunger.org/sites/default/files/publications/Delivering_Money-Cash_Transfer_Mechanisms_in_Emergencies_03.2010.pdf [1 May 2018].

Hosein, G. 2011. *Privacy and developing countries*, Privacy Research Papers, Office of the Privacy Commissioner of Canada. Available at: https://priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2011/hosein_201109/ [1 May 2018].

—; Nyst, C. 2013. *Aiding Surveillance: An Exploration of How Development and Humanitarian Aid Initiatives are Enabling Surveillance in Developing Countries*, Privacy International.

ICHRP (International Council on Human Rights Policy). 2010. *Modes and Patterns of Social Control. Implications for Human Rights Policy* (Geneva).

ISPA (Inter Agency Social Protection Assessments). 2016. *Identification systems for social protection*. *"What Matters" Guidance Note* (Washington, DC, Inter Agency Social Protection Assessments Partnership). Available at: http://www.ispatools.org [27 Apr. 2018].

ILO (International Labour Office). 2015. "A national health insurance beneficiary registry based on national identification numbers: Thailand", *Building Social Protection Floors Brief* (Geneva).

—. 2017a. *Building social protection systems: International standards and human rights instruments* (Geneva).

—. 2017b. *World Social Protection Report 2017–19: Universal social protection to achieve the Sustainable Development Goals* (Geneva).

—; OPM (Oxford Policy Management). 2014. *Report to the Government: Namibia social protection floor assessment report* (Pretoria).

Kidd, S. 2016. *To condition or not to condition: What is the evidence?* Pathways' perspectives on social policy in international development, Issue No. 20 (Kent, Development Pathway).

LaMonica, M. 2014. *Fingerprinting infants helps track vaccinations in developing countries*, blog posted in MIT Technology Review, 4 September 2014. Available at: https://www.technologyreview.com/s/530481/fingerprinting-infants-helps-track-vaccinations-in-developing-countries/ [1 May 2018].

Lindskov Jacobsen, K. 2017. "On Humanitarian Refugee Biometrics and New Forms of Intervention", in *Journal of Intervention and Statebuilding*, Vol. 11 Issue 4, 529-551, DOI: 10.1080/17502977.2017.1347856.

Lyon, D. 2007. "National ID Cards: Crime-Control, Citizenship and Social Sorting", in *Policing: A Journal of Policy and Practice*, Vol. 1, Issue 1, pp. 111-118. Available at: https://doi.org/10.1093/police/pam015 [11 May 2018].

McKee, K. 2012. *What if poor people do care about privacy of their financial data*, blog posted on 6 December 2012, The Consultative Group to Assist the Poor (CGAP). Available at: http://www.cgap.org/blog/what-if-poor-people-do-care-about-privacy-their-financial-data [1 May 2018].

Maqueo-Ramirez, M. S.; Moreno-González, J.; Recio-Gayo, M. 2017. "Protección de datos personales, privacidad y vida privada: la inquietante búsqueda de un equilibrio global necesario", in *Revista de Derecho*, Vol. 30, No. 1, pp. 77-96, DOI: 10.4067/S0718-09502017000100004.

Maldonado, J. H.; Moreno, R. del P.; Giraldo Pérez, I.; Barrera Orjuela, C. A. 2011. *Los programas de transferencias condicionadas: ¿hacia la inclusión financiera de los pobres en América Latina?* (Ottawa, International Development Research Centre).

Nowak, M. 2005. *U.N. Covenant on Civil and Political Rights. CCPR Commentary*, 2nd rev. ed. (Kehl, Germany and Arlington VA, N.P. Engel).

OHCHR (Office of the United Nations High Commissioner for Human Rights). 2011. Guiding principles on business and human rights (New York, United Nations). Available at: http://www.ohchr.org/documents/publications/GuidingprinciplesBusinesshr_en.pdf [9 May 2018].

—. 2014. *The right to privacy in the digital age*, A/HRC/27/37 (New York).

OPM (Oxford Policy Management). 2013. *Evaluation of the Uganda Social Assistance Grants for Empowerment (SAGE) Programme: Baseline Report* (Pretoria).

Rahman, Z. 2017. *Irresponsible data? The risks of registering the Rohingya*, IRIN, Berlin, 23 October 2017. Available at: https://www.irinnews.org/opinion/2017/10/23/irresponsible-data-risks-registering-rohingya [1 May 2018].

Ramanathan, U. 2014. *Biometric use for social protection programmes in India risk violating human rights of the poor*, UNRISD Resource Platform, 2 May 2014. Available at: http://socialprotection-humanrights.org/expertcom/biometrics-use-for-social protection-programmes-in-india-risk-violating-human-rights-of-the-poor/ [1 May 2018].

SASSA (South African Social Security Agency). 2017. *Annual Report 2016/2017* (Pretoria).

Sepúlveda, M.; van Banning, T.; Gudmundsdottir, G.; Chamoun, C.; van Genugten, W. 2004. *Human Rights Reference Handbook*, third rev. ed. (Ciudad Colon, University for Peace).

UNICEF (United Nations Children's Fund). 2012. *Integrated social protection systems: Enhancing equity for children*, UNICEF Social Protection Strategic Framework (New York).

UN (United Nations). 1999. *Consideration of reports submitted by States parties under article 40 of the Covenant. Concluding Observations of the Human Rights Committee*, Canada, CCPR/C/79/Add.105, 7 April 1999 (New York).

World Bank. 2015. *Identification for Development (ID4D) Integration Approach*. Study (Washington, DC).

Additional bibliography consulted

Barca, V.; Hurrell, A.; MacAuslan, I.; Visram, A.; Willis, J. 2010. *Paying attention to detail: How to transfer cash in cash transfers* (Oxford Policy Management). Available at: http://www.chronicpoverty.org/uploads/publication_files/barca_et_al_cash_transfers.pdf [2 May 2018].

Bennett, C. J.; Lyon, D. (eds.). 2008. *Playing the Identity Card: Surveillance, Security and Identification in Global Perspective* (London and New York, Routledge).

Bold, C.; Porteous, D.; Rotman, S. 2012. "Social Cash Transfers and Financial Inclusion: Evidence from Four Countries", *Focus Note* 77 (Washington, DC, CGAP).

Chirchir, R. 2016. *An overview of Kenya's Single Registry Model* (Nairobi, Development Pathways Kenya Ltd.). Available at: http://www.developmentpathways.co.uk/resources/an-overview-of-kenyas-single-registry-model/ [1 May 2018].

Das, J.; Leino, J. 2011. "Evaluating the RSBY. Lessons from an Experimental Information Campaign", in *Economic and Political Weekly*, August 2011, vol. XLVI, No. 32.

Electronic Frontier Foundation (no date): Mandatory National IDs and Biometric Databases. Available at: https://www.eff.org/issues/national-ids [2 May 2018].

Fan, V. 2013. *The Early Success of India's Health Insurance for the Poor, RSBY*, Center for Global Development Essay (Washington, DC, Center for Global Development). Available at: http://www.cgdev.org/sites/default/files/archive/doc/full_text/CGDEssays/3120468/early-success-indias-health-insurance-rsby.html [2 May 2018].

Gelb, A.; Clark, J. 2012. *Building a biometric national ID: Lessons for developing countries from India's Universal ID Program*, Center for Global Development, CGD Brief October 2012 (Washington, DC, Center for Global Development).

Gellman, R. 2013. *Privacy and Biometric ID Systems: An Approach Using Fair Information Practices for Developing Countries*, CGD Policy Paper 28 (Washington, DC, Center for Global. Development). Available at: http://www.cgdev.org/sites/default/files/privacy-and-biometric-ID-systems_0.pdf [2 May 2018].

Government of India. 2014. *Mahatma Gandhi National Rural Employment Guarantee Act 2005, Report to The People* (New Delhi).

Government of Peru. 2010a. *Informe Compilatorio: "El Programa Juntos, Resultados y Retos"*, Presidencia del Consejo de Ministros (Lima). Available at: http://www.juntos.gob.pe/modulos/mod_infojuntos_V1/docs/11.pdf [2 May 2018].

—. 2012. Registro Nacional de Identificación y Estado Civil: Plan Nacional Perú contra la Indocumentación 2011-2015 (Lima). Available at: http://www2.congreso.gob.pe/sicr/cendocbib/con4_uibd.nsf/9CB85613535A717905257C050060EC79/$FILE/plan-nacional-2011-2015.pdf [2 May 2018].

ILO (International Labour Office). 2014. *Cadastro Unico - Operating a Registry through a National Public Bank*, Building Social Protection Floors Brief, No. 1 (Geneva).

Klapper, L.; Singer, D. 2014. *The Opportunities of Digitizing Payments* (Washington, DC, World Bank).

La Rue, F. 2013. *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, A/HRC/23/40 (New York).

Longman, T. 2001. "Documentation and Individual Identity in Africa: Identity Cards and Ethnic Self-Perception in Rwanda", in Jane Caplan and John Torpey, eds., *Documenting Individual Identity: The Development of State Practices in the Modern World* (Princeton, Princeton University Press, pp. 345-357).

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

NIMC (National Identity Management Commission). 2014. 2014 *Annual Report and Accounts*. National Identity Management Commission (Abuja). Available at: http://www.nimc.gov.ng/docs/reports/annual_report_2014.pdf [2 May 2018].

OHCHR (Office of the United Nations High Commissioner for Human Rights). 2014. Birth registration and the right of everyone to recognition everywhere as a person before the law UN Doc. A/HRC/27/22.

O'Neil King, R. 2014. *Banking and Biometrics.* White paper (Biometrics Research Group, Inc. Available at: http://www.biometricupdate.com/wp-content/uploads/2014/12/Biometrics-and-Banking-Special-Report-2014.pdf [6 May 2018].

Paes de Sousa, R. 2005. *Challenges in Monitoring and Evaluation of Social Development Policy*, Secretary of Evaluation and Information Management, Ministry of Social Development and Fight Against Hunger, Brasilia 2005. Available at: http://siteresources.worldbank.org/SAFETYNETSANDTRANSFERS/Resources/281945-1131468287118/1876750-1132152694149/Romulo_Challenges_MandE.pdf [6 May 2018].

Pato, J. N.; Millett, L. I. (eds). 2010. *Biometric Recognition: Challenges and Opportunities* (Washington, DC, The National Academies Press).

Pitula, K.; Sinnig, D.; Radhakrishnan, T. 2009. *Making Technology Fit: Designing an Information Management System for Monitoring Social Protection Programmes in St. Kitts* (Montreal, Concordia University). Available at: http://sta.uwi.edu/conferences/09/salises/documents/D%20Dysart-Gale.pdf [6 May 2018].

Priyanto, U. 2012. "National Electronic ID Card (e-KTP) programme in Indonesia", presentation at the ID World Conference, Abu Dhabi, 18–19 March 2012. Available at: https://www.scribd.com/document/240007853/1-Priyanto-Unggul [6 May 2018].

Reuben, W.; Cuenca, R. 2009. *El estado de la indocumentación infantil en el Perú: Hallazgos y propuestas de política* (Lima, World Bank).

Sepúlveda, M. 2009a. *Report of the United Nations Independent Expert on the question of human rights and extreme poverty,* A/HRC/11/9 (New York, United Nations): on cash transfers programmes and human rights.

—. 2009b. *Report of the United Nations Independent Expert on the question of human rights and extreme poverty*, A/64/279 (New York, United Nations): on social protection system and the financial and economic crisis.

—. 2010a. *Report of the United Nations Independent Expert on the question of human rights and extreme poverty*, A/HRC/14/31 (New York, United Nations): on social protection and old age poverty with specific focus on older women.

—. 2010b. *Report of the United Nations Independent Expert on the question of human rights and extreme poverty,* A/65/259 (New York, United Nations): on the importance of gender sensitive social protection systems in achieving the Millennium Development Goals.

—. Mimeo. *The use of biometric technology in social protection programmes in developing countries: Are we moving in the right direction?*, study submitted to the ILO, unpublished, 2013.

—; Nyst, C. 2012. *The Human Rights approach to social protection*, Elements for Discussion Series (Helsinki, Ministry for Foreign Affairs of Finland).

Setel, P. W.; Macfarlane, S. B.; Szreter, S.; Mikkelsen, L.; Jha, P.; Stout, S.; AbouZahr, C. 2007. "Who Counts? A scandal of invisibility: making everyone count by counting everyone", in *Lancet*, Vol. 370, pp. 1569–77, DOI:10.1016/S0140-6736(07)61307-5.

South African Law Reform Commission. 2005. *Privacy and Data protection*, Discussion Paper 109, Project 124 (Pretoria).

South African Social Security Agency (no date). *You & your new SASSA payment card*. Available at: www.sassa.gov.za [6 May 2018].

UNICEF (United Nations Children's Fund). 2013. *Every Child's Birth Right: Inequities and trends in birth registration* (New York).

United Nations Statistics Division. 2002. *The Handbook on Training in Civil Registration and Vital Statistics Systems* (New York).

Ward, P.; Hurrell, A.; Visram, A.; Riemenschneider, N.; Pellerano, L.; O'Brien, C.; MacAuslan, I.; Willis, J. 2010. *Cash Transfer Programme for Orphans and Vulnerable Children (CT-OVC), Kenya: Operational and Impact Evaluation, 2007-2009* (Oxford Policy Management).

World Bank (no date): "Identification of beneficiaries" in *Safety Nets How to. A toolkit for practitioners* (version 1). Available at: http://siteresources.worldbank.org/SAFETYNETSANDTRANSFERS/Resources/281945-1291746977764/HowtoCompletePdfs.pdf [6 May 2018].

—. 2012. *Resilience, equity and opportunity: The World Bank 2012-2022 Social Protection and Labor Strategy* (Washington, DC).

—. 2015. *The State of Social Safety Nets 2015* (Washington, DC).

—. 2018. *Technology Landscape for Digital Identification* (Washington, DC).

Zimmerman, J. M.; Bohling, K.; Rotman Parker, S. 2014. *Electronic G2P Payments: Evidence from Four Lower-Income Countries*, Focus Note 93 (Washington, DC, CGAP).

Legal cases

- Supreme Court of India. Case of Justice KS. *Puttaswamy (Retd.)* vs. *Union of India and Others*, 24 August 2017.
- Supreme Court of Argentina. Case 1172/03, 26 March 2014.
- Constitutional Court of South Africa. Case *Black Sash Trust* v. *Minister of Social Development and Others (Freedom Under Law NPC Intervening)*, CCT 48/17, 15 June 2017.
- Court of Justice of the European Union. Joined cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and Others, 8 April 2014.
- ECHR (European Court of Human Rights). *Leander* v. *Sweden*, Application No. 9248/81, 26 March 1987.
- ECHR. *Z.* v. *Finland*, Application No. 22009/93, 25 February 1997.
- ECHR. *P.G. and J.H.* v. *the United Kingdom*, Application No. 44787/98, 25 September 2001.
- ECHR. *Peck* v. *the United Kingdom,* Application No. 44647/98, 28 January 2003.
- ECHR. *Perry* v. *the United Kingdom,* Application No. 63737/00, 17 July 2003.
- ECHR. *I.* v. *Finland,* Application No. 20511/03, 17 July 2008.
- ECHR. *S. and Marper* v. *the United Kingdom*, Application Nos. 30562/04 and 30566/04, 4 December 2008.
- ECHR. *M.K.* v. *France*, Application No. 19522/09, 18 April 2013.

Cited domestic legislation

Chile

- Law No. 19.949, which creates the social protection system called Chile Solidario. Adopted 17 May 2004; most recent reform 17 May 2008.
- Law No. 19.628, protection of privacy, 28 August 1999.
- Decree No. 235, which regulates implementation of Chile Solidario, 25 November 2004.

India

- The National Rural Employment Guarantee Act, No. 42 of 5 September 2005.
- The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, No. 18 of 25 March 2016.

Mexico

- Official Decree of 30 December 2014, which establishes the Operational Rules of the Prospera program.
- Federal Transparency and Access to Public Government Information Act, 9 May 2016.
- National Statistics and Geographic Information Act, 12 December 1983.

South Africa

- Protection of Personal Information Act, No. 4 of 2013.
- Social Assistance Act, No. 13 of 2004.

United Kingdom

- Data protection (Processing of Sensitive Personal Data) Order 2000, No. 417, 17 February 2000.