



DATA PROTECTION AND PRIVACY FOR SOCIAL ASSISTANCE BENEFICIARIES: A SOUTH AFRICAN PERSPECTIVE

Ntando Ncamane

Abstract

Social Security plays a significant role in South Africa by ensuring that everyone has the right to social assistance, as enshrined in section 27 of the Constitution. In realising this right the legislature enacted the Social Assistance Act and the South African Social Security Agency Act, in which the former makes provisions for the different type of social assistance and the latter provides for the establishment of the SASSA, an institution responsible for the administration and payment of social assistance. Owing to the forever-evolving technology and the convenience it sometimes brings, the agency decided to migrate to digital payments of social assistance through SASSA master cards. In terms the law, the state is under the obligation to ensure that it protects personal information belonging to social assistance beneficiaries which is required by state for purpose of processing. The state is also under the obligation to guard against any illegal use of social assistance beneficiaries personal data. However, during the migration to digital payment SASSA breached laws which protects the data and privacy of the beneficiary. This is also evident in the landmark case of *Black Sash Trust v Minister of Social Development*, which validated the importance of the beneficiary's privacy and data protection. To this effect, the court ordered that the state, in particular SASSA, has a duty to protect information belonging to the social assistance beneficiaries and should devise measures that will protect personal information and deter any possible breach or illegal use. This chapter recommends sound and practical measures that can be adopted by the state so to circumvent any possible breach and illegal use of personal information belonging to social assistance beneficiaries.

1 Introduction

One of the signature achievements of our constitutional democracy is the establishment of an inclusive and effective programme of social assistance. It has had a material impact in reducing poverty and inequality and in mitigating

the consequences of high levels of unemployment. In so doing, it has given some content to the core constitutional values of dignity, equality.¹

The Constitution of the Republic of South Africa² makes provision for everyone to have the right of access to social assistance.³ This right falls under the socio-economic category of rights, among others, the rights to adequate food, water and social security.⁴ In *Government of the Republic of South Africa & Others v Grootboom & Others (Grootboom)*⁵ it was held that socio-economic rights are targeted at the vulnerable, and that government policies must be aligned to address socio-economic rights-related issues.⁶ The Court further stated that if the state has programmes in place to provide social assistance to citizens, the state has realised its obligation to realise socio-economic rights.⁷ In a bid to realise and distribute social assistance, the legislature has enacted the Social Assistance Act 13 of 2004,⁸ which provides for the rendering of social assistance services that the administration and payment of social grants.⁹ The South African Social Security Agency Act 9 of 2004¹⁰ was also enacted, giving rise to the establishment of the South African Social Security Agency with the duty to administer and monitor social grant payments.¹¹

South African technology has over the years evolved, and the South African Social Security Agency (SASSA) has been a beneficiary of these technological developments, such as the digitisation of payment of social grants, which included the introduction of smart cards, referred to as SASSA master cards. This endeavour was also meant to eliminate fraud related to the payments of social grants.¹² As a result, the services of cash payment services (CPS) were sourced to distribute social grant payments. The processing of payments requires the details of beneficiaries, and to

1 *Black Sash Trust v Minister of Social Development & Others (Freedom Under Law NPC Intervening)* (CCT48/17) [2017] ZACC 20; 2017 (9) BCLR 1089 (CC) (15 June 2017) para 1.

2 Constitution of the Republic of South Africa, 1996.

3 Sec 27(1)(c) Constitution.

4 Sec 27 Constitution.

5 2001 (1) SA 46 (CC).

6 *Grootboom* (n 5) para 36.

7 As above.

8 Social Assistance Act 13 of 2004.

9 Sec 3 Social Assistance Act.

10 South African Social Security Agency Act 9 of 2004.

11 Sec 2 South African Social Security Agency Act.

12 <https://www.gov.za/ten-million-sassa-mastercard-cards-issued-south-african-social-grant-beneficiaries> (accessed 15 September 2020).

protect their personal data and privacy, a legal framework was put in place to protect these beneficiaries from the illegal use of their personal information. The first of its kind is section 14 of the Constitution,¹³ which bestows the right privacy on everyone.¹⁴ The Protection of Personal Information Act 4 of 2013¹⁵ was enacted for public and private institutions to promote the protection of personal information. Furthermore, the South African Social Security Agency Act makes provision for SASSA to protect confidential information at its disposal.¹⁶ The duty of SASSA to provide adequate safeguards was confirmed in the landmark case of *Black Sash Trust v Minister of Social Development*.¹⁷ It further stated that it

contains adequate safeguards to ensure that personal data obtained in the payment process remains private and may not be used for any purpose other than payment of the grants or any other purpose sanctioned by the Minister in terms of section 20(3) and (4) of the Social Assistance Act 13 of 2004 ... Preclude anyone from inviting beneficiaries to 'opt-in' to the sharing of confidential information for the marketing of goods and services.¹⁸

The state's onerous endeavour to put in place a legal framework to enable the protection of personal data and privacy of social grant beneficiaries is commendable and has ameliorated the social assistance digitalised payment system. However, some notable shortcomings remain, which may defeat the purpose of the aforementioned legal measures that aim at the protection of beneficiaries. The first is non-compliance with the order of the Constitutional Court, also highlighted by the Black Sash that discovered, when making submissions to the UN General Assembly, that personal information that belongs to beneficiaries is still withheld by Net1, which contracted to CPS,¹⁹ which is contrary to the order of the Court quoted above. An article by Prinsloo and Ntondini suggests that there are still numerous cases of social grant personal data and privacy being used and, as a result, there are discrepancies in amounts paid to these beneficiaries.²⁰ Lastly, the SASSA and the South African Post Office (the new distributors of grants) personnel have not been fully acquainted with

13 Sec 14 Constitution.

14 Sec 14(1) Constitution.

15 Protection of Personal Information Act 4 of 2013.

16 Sec 16 SASSA Act .

17 *Black Sash Trust* (n 1).

18 *Black Sash Trust* (n 1) paras 76, 10.1.

19 Black Sash Submission UN General Assembly on Digital Technology, Social Protection and Human Rights 2019.

20 T Prinsloo & S Ntondini 'The exploitation of South African Social Security Agency grant recipients' data' (2006) *International Journal of Social Welfare* 16.

this new system, resulting in maladministration enabling cyber criminals to gain access to personal data of beneficiaries. This does not only have a negative impact on beneficiaries' personal data but also denies them the right to social assistance.²¹

It is against this background that this chapter will first examine the regulation of social assistance, in particular section 27(1)(c) of the Constitution,²² the Social Assistance Act 13 of 2004²³ and the South African Social Security Agency Act 9 of 2004,²⁴ which gave rise to the establishment of SASSA as the sole agency responsible for the payment of social assistance grants.²⁵ This chapter will further examine the laws put in place to protect social grant beneficiaries against the illegal use of data and the infringement of their privacy. These laws include section 14 of the Constitution,²⁶ which guarantees everyone the right to privacy. It will further examine the state's duty, in particular SASSA's duty, to implement safety measures in order to protect personal data and the privacy of social assistance beneficiaries when making payments, in light with the above-mentioned statutes. A brief analysis of the *Black Sash Trust* case²⁷ will be analysed as it contains safety measures to protect information pertaining to social assistance beneficiaries against the illegal use of their personal information. This safety is also extended to third parties who have been awarded a tender to render social assistance payments, which would require the personal details of the beneficiaries in order to effect payment. Lastly, the chapter will recommend solutions to the shortcomings associated with cash payment system inadequacies of beneficiaries' personal data and privacy.

2 Regulation of social assistance

Social assistance enjoys regulation and protection from the Constitution as well as other statutes, such as the Social Assistance Act and South African Social Security Agency Act. It is imperative for this study to first briefly define the terms 'social security' and 'social assistance' to gain a better understanding of the discussion that will follow.

21 B Batchelor & T Wazvaremhaka 'Balancing financial inclusion and data protection in South Africa: *Black Sash Trust v Minister of Social Development* 2017 (9) 1089 (CC)' (2019) 136 *South African Law Journal* 129.

22 Sec 27(1)(c) Constitution.

23 Social Assistance Act 13 of 2004.

24 South African Social Security Agency Act 9 of 2004.

25 Sec 2 South African Social Security Agency Act.

26 Sec 14 Constitution.

27 *Black Sash Trust* (n 1).

Social Assistance is defined in the White Paper on Social Welfare as ‘non-contributory and income-tested benefits provided by the state to groups such as people with disabilities, elderly people and unsupported parents and children who are unable to provide for their own minimum needs’.²⁸

In South Africa, social assistance has taken the form of social grants. Social assistance is a stream of social security law, which is defined by the International Labour Organisation (ILO) as ‘the protection that a society provides to individuals and households to ensure access to health care and to guarantee income security, particularly in cases of old age, unemployment, sickness, invalidity, work injury, maternity or loss of a breadwinner’.²⁹

Among the streams of social security there are other streams such as social insurance, social relief and private saving, which feeds up to the broad scope and purpose of social security law. Social security is covered by section 27 of the Constitution,³⁰ which means that social assistance has since enjoyed constitutional protection afforded in the new democratic dispensation. Section 27 of the Constitution³¹ reads as follows:

- (1) Everyone has the right to have access to –³²
 - (a) healthcare services, including reproductive health care;³³
 - (b) sufficient food and water³⁴; and
 - (c) social security, including, if they are unable to support themselves and their dependants, appropriate social assistance.³⁵
- (2) The state must take reasonable legislative and other measures, within its available resources, to achieve the progressive realisation of each of these rights.³⁶

28 Department of Welfare *White Paper for Social Welfare: Principles, guidelines, recommendations, proposed policies and programmes for developmental social welfare in South Africa* (1997) 50.

29 https://www.ilo.org/wcmsp5/groups/public/---dgreports/dcomm/documents/publication/wcms_067588 (accessed 15 September 2020).

30 Sec 27 Constitution.

31 As above.

32 Sec 27(1) Constitution.

33 Sec 27(1)(a) Constitution.

34 Sec 27(1)(b) Constitution.

35 Sec 27(1)(c) Constitution.

36 Sec 27(2) Constitution.

(3) No one may be refused emergency medical treatment.³⁷

The focal point of this study is on section 27(1)(c) which bestows on everyone the right to social assistance who is unable to support themselves, including their dependants. The state is required to take reasonable legislative measures within its resources to address social assistance concerns. The *Grootboom* case³⁸ acknowledges the dire need for the state to address socio-economic conditions in our societies as a result of the severe injustices of the past.³⁹ However, the Court was cognisant of the fact that the state might not be able to go beyond its limited resources in a bid to address socio-economic needs or to immediately realise these socio-economic rights. Notwithstanding the limitation on the realisation of socio-economic rights, the Court held that this was an explicit obligation and that the courts should at all times enforce these rights to enable the realisation of the rights.⁴⁰ The Constitutional Court in the case of *Khosa v The Minister of Social Development & Others; Mahlaule & Others v The Minister of Social Development & Others*⁴¹ highlighted the importance of social security but in particular social assistance, that the primary purpose of social assistance is that the state values human beings and it is to a social intervention for citizens to afford the basic life that they are not able to afford.⁴² To give effect to the constitutional mandate of the state, which is to provide social assistance, the legislature enacted the Social Assistance Act 9 of 2004⁴³ and the South African Social Security Agency 3 of 2004.⁴⁴ These two legislations had a tremendous impact towards the development of South African social assistance system. The Social Assistance Act was aimed at providing for the payment of social assistance grants and to outline the minimum requirements for persons to qualify for social assistance grants. The Act made provision for social assistance payments to be paid in terms of a child support grant;⁴⁵ a dependency grant,⁴⁶ a

37 Sec 27(3) Constitution.

38 *Grootboom* (n 5).

39 *Grootboom* (n 5) para 93.

40 *Grootboom* (n 5) para 94.

41 2004 (6) BCLR 569 (CC).

42 As above.

43 Social Assistance Act 9 of 2004.

44 South African Social Security Agency 3 of 2004.

45 Sec 4(a) Social Assistance Act.

46 Sec 4(b) Social Assistance Act.

foster child grant;⁴⁷ a disability grant;⁴⁸ an older person's grant;⁴⁹ a war veteran's grant;⁵⁰ and a grant-in-aid.⁵¹ Each category of social grant had its own eligibility requirements. The Act empowered the agency to make payments to persons who have submitted relevant information and meet the stipulated requirements. Primary to the South African Social Assistance Act was the provision for SASSA, which was entrusted with the responsibility of administrating and paying social grant payments.

3 Regulatory framework to protect data and privacy of beneficiaries

3.1 International instruments

Sweden is regarded as the first country in the universe to enact data protection laws dating back to 1973. However, in the mid 1980s data protection was a global phenomenon as a result of there being a rapid emergence of the global market, leading to an increase in the exchange of personal information. This encouraged many international organisations to enact international instruments that will give rise to the protection of data and privacy.⁵² To regulate and provide guidance nations on matter of data protection and privacy, international organisations such as the Organisation for Economic Cooperation and Development (OECD), the European Council and the European Economic Community (now the European Union) (EU) came up with documents aimed at developing standard international data protection laws and to enable the free flow of information and also to archive uniform national laws on data protection and privacy.⁵³ The European countries under the Europe Council were the first to develop and enhance data protection and privacy laws. This is why many countries around the world draw lessons from EU countries, in particular the United States.⁵⁴

In 1990 the United Nations General Assembly (UNGA) adopted the Guidelines for the Regulation of Computerised Personal Data Files. The Guide provided the procedures for the implementation and proper

47 Sec 4(c) Social Assistance Act.

48 Sec 4(d) Social Assistance Act.

49 Sec 4(e) Social Assistance Act.

50 Sec 4(f) Social Assistance Act.

51 Sec 4(g) Social Assistance Act.

52 A Roos 'Core principles of data protection law' (2006) 39 *Comparative and International Law Journal of Southern Africa* 103.

53 As above.

54 Roos (n 52) 105.

guidance on data protection on national legislation of member states.⁵⁵ The Guidelines outline minimum guarantees to which member states should adhere. These minimum guarantees are the principle of lawfulness and fairness; the principle of accuracy; the principle of the purpose-specification; the principle of interested person access; the principle of non-discrimination; the power to make exceptions; the principle of security; supervision and sanctions; trans-border data flows; and fields of application.⁵⁶ However, the focal point of this chapter rather is on African data protection-related instruments. Hence there will be no further deliberation on EU instruments as this will serve no purpose.

The Social Protection Floors Recommendation 202 of 2012 was enacted to give guidance to member states to develop a comprehensive social security and extend social security coverage.⁵⁷ The Recommendation mandates member states to establish legal frameworks that will ensure that data of social security beneficiaries is legally protected.⁵⁸

Moreover, at the continental level, the African Union (AU), in a bid to curb cybercrimes and to protect personal data, has enacted the African Union Convention of Cyber Security and Personal Data Protection which was adopted in 2014.⁵⁹ The Convention comes after protracted deliberation from the first extraordinary meeting of African ministers who were responsible for communications resolute on a declaration that was directed at the AU to develop a continental cybersecurity and personal data protection as well as any other relevant needs of the continent. The Convention was adopted by the AU heads of state in 2014.⁶⁰ Chapter 2 of the Convention deals in detail with the regulation of personal data.⁶¹ As part of the Convention's objectives it encourages state parties to commit to establishing a legal framework that enhances the protection of personal data and to sanction those who breach privacy protection laws, without impeding the free flow of personal information.⁶² The Convention makes

55 UN General Assembly Guidelines for the Regulation of Computerized Personal Data Files, 14 December 1990, <https://www.refworld.org/docid/3ddcafaac.html> (accessed 27 November 2020).

56 As above.

57 Preamble to the Social Protection Floors Recommendation 2012 (No 202).

58 IV Monitoring of the Social Protection Floors Recommendation, 2012 (No 202) para 23.

59 African Union Convention of Cyber Security and Personal Data Protection 2014.

60 UJ Orji *The African Union Convention on Cybersecurity: A regional response towards cyber stability?* (2018) 98.

61 Ch 2 Personal Data Protection.

62 Art 8(1) African Union Convention of Cyber Security and Personal Data Protection 2014.

provision for member states to establish institutional frameworks for the protection of personal data.⁶³ The national authority of personal data is therefore tasked with the responsibility of being impartial and independent, which will ensure that data processing complies with the provisions of the African Union Convention of Cyber Security and Personal Data Protection.⁶⁴

The Convention goes further by outlining governing principles to the processing of data. It lists a number of principles, namely, the principle of consent and legitimacy of personal data processing;⁶⁵ the principle of lawfulness and fairness of personal data processing;⁶⁶ the principle of purpose, relevance and storage of processed personal data;⁶⁷ the principle of accuracy of personal data;⁶⁸ the principle of transparency of personal data processing;⁶⁹ the principle of confidentiality; and security of personal data processing.⁷⁰ The person, among other obligations owing to the data subject, the data controller, has an obligation to keep the processing of data confidential and the processing shall be performed by a person operating under the instruction of the personal data controller.⁷¹ The data controller is required to take all precautionary possible measures to ensure that personal data belonging to the data subject is not extinguished or tampered with by non-authorised persons.⁷² To amplify the protection of data and privacy in Africa, the Convention mandates the African Union Commission to develop guidelines on personal data protection. The guides were developed together with the Internet Society as well experts in the field of data protection and privacy, including privacy specialists,

63 Art 11(1) African Union Convention of Cyber Security and Personal Data Protection 2014.

64 As above..

65 Art 13, Principle 1 African Union Convention of Cyber Security and Personal Data Protection 2014.

66 Art 13, Principle 2 African Union Convention of Cyber Security and Personal Data Protection 2014.

67 Art 13, Principle 3 African Union Convention of Cyber Security and Personal Data Protection 2014.

68 Art 13, Principle 4 African Union Convention of Cyber Security and Personal Data Protection 2014.

69 Art 13, Principle 5 African Union Convention of Cyber Security and Personal Data Protection 2014.

70 Art 13, Principle 6 African Union Convention of Cyber Security and Personal Data Protection 2014.

71 Art 20 African Union Convention of Cyber Security and Personal Data Protection 2014.

72 Art 21 of the African Union Convention of Cyber Security and Personal Data Protection 2014.

academics and civil society groups.⁷³ The guidelines put an emphasis on ensuring that trust is paramount on online services to enable the digital economy to be beneficial and productive. The guidelines further emphasised the need for countries to create proactive measures so as to guard citizens against the victimisation of their personal data and to not disregard the role of other stakeholders in this regard.⁷⁴

Greenleaf and Cottier submit that Africa has made significant progress with regard to the advancement of the data protection laws. This is proven by the fact that the enactors of international instruments and national laws relating to data protection are countries in the European Council,⁷⁵ but Africa is leading on the expansion of data laws, which is evident from the fact that 12 countries have since 2013 adopted new laws. Most African countries have been first to apply to the European Council to be accepted to accede. Therefore, these factors should be evidence enough to prove data protection progression in Africa.⁷⁶

3.2 Constitution of the Republic of South Africa

The legal point of departure in the protection of data and privacy is the constitutional protection afforded to all beneficiaries of social assistance grants. Following the new democratic dispensation, the Constitution is viewed as being the supreme law and any law or act inconsistent with it is invalid.⁷⁷ The Bill of Rights, as the cornerstone of our democracy, guarantees everyone the right to privacy, which is the crucial right for purposes of this chapter. The case of *Bernstein v Bester*⁷⁸ remains a leading case that deals with the overall aspects of the right to privacy as far as South African jurisprudence is concerned. The case drew most of its inferences from foreign law to denote two fundamental approaches that should be taken into account where there is a dispute pertaining to the right to privacy. However, these approaches were based on what is termed as 'legitimate expectations'. The Constitutional Court held that 'it seems to be a sensible approach to say that the scope of a person's privacy

73 Privacy and Personal Data Protection Guidelines for Africa, https://www.internetsociety.org/wp-content/uploads/2018/05/AUCPrivacyGuidelines_2018508_EN.pdf (accessed 2 December 2020).

74 As above.

75 G Greenleaf & B Cottier 'Comparing African data privacy laws: International, African and regional commitments' University of New South Wales Law Research Series, 2020 4.

76 Greenleaf & Cottier (n 75) 5.

77 Sec 2 Constitution.

78 1996 (2) SA 751 (CC)

extends *a fortiori* only to those aspects in regard to which a legitimate expectation of privacy can be harboured'. Therefore, the right to privacy is recognised as having two components, namely, that the person must have a subjective expectation of privacy, and that society must have recognised the expectation as objectively reasonable.

Section 32 of the Constitution⁷⁹ in chapter 2 of the Bill of Rights also becomes relevant for the purposes of this chapter. Section 32 reads as follows:

- (1) Everyone has the right of access to –⁸⁰
 - (a) any information held by the state; and⁸¹
 - (b) any information that is held by another person and that is required for the exercise or protection of any rights.⁸²
- (2) National legislation must be enacted to give effect to this right, and may provide for reasonable measures to alleviate the administrative and financial burden on the state.⁸³

In this regard the most relevant provision is section 2 which empowers National Assembly to enact legislation that will give effect to section 32. The essence and relevance of this provision will be discussed later in this chapter. However, the importance of this provision is noted by Ngcobo J in the case of *Brümmer v Minister for Social Development & Others*⁸⁴ in which he affirms the significance of this right, more so in country found on the principles of values of accountability, responsiveness and openness cannot be overlooked.⁸⁵ Peekhaus argues that South Africa is one of the new countries that have made positive progress in enhancing the right to access information.⁸⁶

3.3 Common law

Before the right to privacy was validated by the Constitution, it found its origin from common law. To date the right still enjoys the common law protection as the common law still recognises the right to privacy. A

79 Sec 32 Constitution.

80 Section 32(1) the Constitution.

81 Sec 32(1)(a) Constitution.

82 Sec 32(1)(b) Constitution.

83 Sec 32(2) Constitution.

84 2009 (6) SA 323 (CC).

85 *Brümmer* (n 84) para 63.

86 W Peekhaus 'South Africa's Promotion of Access to Information Act: An analysis of relevant jurisprudence' (2014) 4 *Journal of Information Policy* 570.

person whose right to privacy has been infringed has recourse in terms of common law to remedy the breach in terms of the *actio iniuriarum*.⁸⁷ If any patrimonial loss is suffered as a result of the infringement of the right to privacy, that person may seek reimbursement in terms of the common law remedy of the *actio legis Aquiliae*. If there is an imminent threat to one's privacy, he or she may apply for an interdict, which is also a common law remedy.⁸⁸ Privacy therefore relates to information, which pertains to an individual who has made a determination that such information to not be revealed to the public. In essence, someone's privacy can be infringed when their facts are made known to the public without their will. Roos submits that this can take two forms. The first is when the outsider took the initiative to learn about the person's facts, which is known as privacy intrusion or acquaintance, or when someone discloses such information to a third party.⁸⁹

3.4 Statutory data protection and privacy

Precisely four known privacy legislations encompass provisions relating to the protection of data and privacy, which are also applicable to social assistance beneficiaries in cases where their data has been illegally used and their privacy has been infringed. Judging from the purpose and nature of these statutes they were enacted to give effect to section 14 of the Constitution, subsequently expanding the protection of data and privacy. The Electronic Communications and Transactions Act 25 of 2002⁹⁰ was intended to regulate electronic communication and also provided for the prevention of the abuse of information.⁹¹ The Act deals with information obtained through electronic transactions and prohibits the data controller from using information without the written permission⁹² of the data subject,⁹³ and it also requires the data controller⁹⁴ to use the data for the purpose for which it was requested.⁹⁵ The Protection of Personal

87 I Currie & J de Waal *The Bill of Rights handbook* (2016) 295.

88 A Roos 'Personal data protection in New Zealand: Lessons for South Africa?' (2008) 11 *Potchefstroom Electronic Law Journal* 90.

89 As above.

90 Electronic Communications and Transactions Act 25 of 2002.

91 Aim of the Electronic Communications and Transactions Act 25 of 2002.

92 Sec 51(1) ECTA.

93 The ECTA defines the data subject as 'mean[ing] any natural person from or in respect of whom personal information has been requested, collected, collated, processed or stored, after the commencement of this Act'.

94 The ECTA defines data controller as follows: "'Data controller" means any person who electronically requests, collects, collates, processes or stores personal information from or in respect of a data subject.'

95 Sec 51(2) ECTA.

Information Act 4 of 2013 (POPIA)⁹⁶ is another legislative measure and it is regarded as the primary legislation aimed at promoting the protection of personal information processed by public and private bodies. It goes further in establishing the minimum standards that apply to the processing of information, and its Preamble recognises the significance of the right to privacy as entrenched in section 14 of the Constitution.⁹⁷ POPIA applies to all information processed entered into the record⁹⁸ and requires persons who are in possession of information belonging to someone else to take proactive measures in protecting that information and maintaining confidentiality.⁹⁹ These proactive steps must be put in place to preclude the loss or damage to or even unauthorised access to the personal information concerned.¹⁰⁰

POPIA¹⁰¹ was enacted to give effect to section 32 of the Constitution, therefore ensuring that everyone exercise their right to access information held by the state.¹⁰² The said Act applies to both private and public bodies.¹⁰³ There is a close juxtaposition between the protection of data and access to information. Both these types of rights complement one another because as much the Constitution affords one with the right to access information, it also affords one protection against the infringement of the right to privacy.¹⁰⁴ The Act warrants the information officer to refuse the disclosure of information that belongs to the third if the disclosure can be viewed as unreasonable, or if the person is deceased.¹⁰⁵ POPIA further

96 Protection of Personal Information Act 4 of 2013 (POPIA).

97 Preamble to the Protection of Personal Information Act 4 of 2013.

98 Sec 3 POPIA.

99 Sec 19(1) POPIA.

100 Sec 19(1)(a)-(b) POPIA.

101 POPIA (n 96).

102 Preamble to the Promotion of Access to Information Act 2 of 2002 (PAIA).

103 Sec 3 PAIA.

104 D van der Merwe *Information and communication technology law* (2016) 25.

105 Sec 34 PAIA. Information officer is defined as “‘information officer’ of, or in relation to, a public body (a) in the case of a national department, provincial administration or organisational component (i) entioned in Column 1 of Schedule 1 or 3 to the Public Service Act, 1994 (Proclamation 103 of 1994), means the officer who is the incumbent of the post bearing the designation mentioned in Column 2 of the said Schedule 1 or 3 opposite the name of the relevant national department, provincial administration or organisational component or the person who is acting as such; or (ii) not so mentioned, means the Director-General, head, executive director or equivalent officer, respectively, of that national department, provincial administration or organisational component, respectively, or the person who is acting as such; [sub-para (ii) amended by s 21 of Act 42 of 2001 (wef 7 December 2001).] (b) in the case of a Municipality, means the municipal manager appointed in terms of section 82 of the Local Government: Municipal Structures Act, 1998 (Act 117 of 1998), or the person who is acting as

prohibits the use or disclosure of certain confidential information as well as other related information.¹⁰⁶ POPIA empowers the information officer to decline the disclosure of the information if the information was submitted in confidence by the third party.¹⁰⁷ The legislature has also incorporated provisions that are important for the personal protection of data belonging to grant beneficiaries in the SASSA Act. This evident from section 16 of the SASSA Act which prohibits SASSA from disclosing social grant personal information that was used for purposes of applying for a social grant. However, this is subject to the provisions of the Constitution or POPIA. This clause makes an exception where there is a court order compelling the agency to disclose or where the beneficiary has consented to such.¹⁰⁸

The Agency has done little in a bid to protect social grant beneficiaries' information. Nonetheless, the Constitutional Court is to be commended for compelling the state to put in place adequate safeguard measures to protect beneficiaries' data being illegally used and their privacy right infringed. This may be viewed as an extension of the existing personal protection laws for social grant beneficiaries. Adequate safeguard measures as a means to protect the rights of social grant beneficiaries were stressed out in the *Black Sash* case.¹⁰⁹ The case concerned a middle man called Cash Paymaster Services that was awarded a tender to render social assistance payments for five years, but the tender was found to be constitutionally invalid.¹¹⁰ The Court suspended the declaration of invalidity, based on the premise that either the tender will be awarded fairly after following the proper procurement process, or SASSA will render payments of social grants itself. SASSA decided not to be awarded the tender and to render payment itself. Unfortunately the agency was not able to meet the deadline and no proactive steps were taken by either the agency or the Minister of Social Development to inform the Constitutional Court timeously about its inability to carry out social grant payments.¹¹¹

This case comes after the 2013 judgment, which declared the CPS contract to be invalid and ordered SASSA to conduct a new procurement process or render payments itself. SASSA's failure, together with that of

such; or (c) in the case of any other public body, means the chief executive officer, or equivalent officer, of that public body or the person who is acting as such.'

106 Sec 31 PAIA

107 Section 31(1)(a) PAIA.

108 Sec 16 SASSA Act.

109 *Black Sash Trust* (n 1).

110 *Black Sash Trust* (n 1) para 3.

111 *Black Sash Trust* (n 1) para 6.

the Minister, led to Black Sash reproaching the Court on the basis of the state's non-compliance with the 2013 court order. Chief among the orders that were made by the Court was that personal information that belonged to the beneficiaries should remain with SASSA and only be utilised for social grants payments.¹¹² The Black Sash Trust applied for direct access on an urgent basis. Black Sash further sought for the following orders:

- (a) that SASSA must file a report on affidavit on how it intends to deal with an interim contract with CPS for payment of social grants from 1 April 2017;
- (b) declaring that CPS is under a duty to act reasonably in negotiating that contract with SASSA;
- (c) that the contract must contain adequate safeguards for various aspects of the personal privacy, dignity and autonomy of grant beneficiaries;
- (d) that the Minister and SASSA must file continuous reports with the Court on the steps taken and to be taken to ensure that payment of social grants is made from 1 April 2017; and
- (e) declaring that SASSA is under a duty to ensure that the payment method must contain adequate safeguards for various aspects of the personal privacy, dignity and autonomy of grant beneficiaries.¹¹³

In light of the above prayers of the applicant, the Court granted the application for direct access, Freedom Under Law was granted leave to intervene and Corruption Watch and the South African Post Office were admitted as friends of the court. The Court further declared that SASSA was under a constitutional obligation to make social grants payments; the suspension on the invalidity of the CPS contract was extended; and CPS as well as SASSA were required to ensure that payment of social assistance grants was effected. The contract was to remain intact and invariable. The Court furthermore ordered that the contract contains provisions that will outline safeguard measures that will enable the safety of personal data of beneficiaries so that it is used for payment purposes only. It was further held that the contract also contains a provision that will prevent inviting beneficiaries in opt-in opt-out or disclose their information for marketing purposes, which was also declared as SASSA's duty to do so.

This case seems to have paved the way for the state's duty, in particular that of SASSA, to ensure that safety measures are put in place that protect data belonging to social grant recipients and prohibit the invasion of their privacy. The case still finds expression and relevancy even in today's social

112 *AllPay Consolidated Investment Holdings (Pty) Ltd v Chief Executive Officer, South African Social Security Agency* ZACC 42; 2014 (1) SA 604 (CC).

113 *Black Sash Trust* (n 1) para 23.

assistance set-up, alongside with the provisions of POPIA and any other relevant statute that may be used in protecting social assistance beneficiaries. It is worth mentioning that POPIA is the most preferred legal avenue to explore in cases of privacy breach of social assistance beneficiaries. This is not to disregard the existing laws that directly or indirectly feed up to the purpose and intention of section 14 of the Constitution.¹¹⁴ However, POPIA¹¹⁵ displays the shortcomings in the existing legislations including the SASSA Act¹¹⁶ and the SAA.¹¹⁷

The provisions relating to data protection and the right to privacy are made enforceable through the Information Regulator, an institution established in terms of section 39 of POPIA.¹¹⁸ The Information Regulator has jurisdiction across the country;¹¹⁹ it is impartial¹²⁰ and is required to function in accordance with the Constitution, POPIA,¹²¹ and is accountable to the legislature.¹²² The Regulator is entrusted with the role of monitoring compliance with the Act by both the private and public sectors; this therefore means that the Act is applicable to SASSA and contracted companies.

4 Challenges

There is no doubt that there has been impactful progress in the South African social assistance arena, with two fundamental legislations being promulgated to regulate the social assistance industry, namely, the Social Assistance Act¹²³ and South African Social Security Agency Act.¹²⁴ These developments necessitated the amelioration of the social assistance system in terms of the digitisation and social grant payments. This is evident in the year 2012 when SASSA introduced electronic payments via the SASSA MasterCard, which initiative was intended to reduce fraud and the possible cost of disbursement.¹²⁵ With the evolving technology

114 Sec 14 Constitution.

115 POPIA (n 96).

116 SASSA Act.

117 Social Assistance Act.

118 Sec 39 POPIA.

119 Sec 39(a) POPIA.

120 Sec 39(b) POPIA.

121 Sec 39(c) POPIA.

122 Sec 39(d) POPIA.

123 Social Assistance Act.

124 South African Social Security Agency Act.

125 AB Fanta and others 'Digitisation of social grant payments and financial inclusion of grant recipients in South Africa – Evidence from FinScope surveys' (2017) *Social Security Review 2*.

across the country and SASSA being no exception to this, there was a dire need for new laws and the amendment of the existing laws so as to protect possible victims against cybercrimes or fraud. Hence, the enactment of the above statutes such as POPIA, ECTA and the SASSA Act as well as the landmark case of *Black Sash*, which enunciated the need for SASSA to implement safety measures that will enable data protection and privacy when contracting with third parties to render payment services to recipients of social assistance grants.

Notwithstanding some of the highlighted developments that have thus far taken place, there are still some glaring challenges faced by SASSA, ultimately affecting social grants beneficiaries, and what is even detrimental is that social assistance beneficiaries are vulnerable people. The first challenge is beneficiaries' information, which still in the possession of Net1 that refuses to return the information.¹²⁶ These allegations were brought forward by Black Sash when it was called upon to make submissions at the United Nations General Assembly on digital technology, social protection and human rights. Furthermore, Net1 has been linked with a company called EasyPay Everywhere, which has low bank charges and has recruited largely social grants beneficiaries, raising concerns after Net1 refused to submit information at its disposal, which might have been used in this process.¹²⁷ This occurred despite the standing order of the Constitutional Court, which states:

The terms and conditions shall:

- (a) contain adequate safeguards to ensure that personal data obtained in the payment process remains private and may not be used for any purpose other than payment of the grants or any other purpose sanctioned by the Minister in terms of section 20(3) and (4) of the Social Assistance Act 13 of 2004; and
- (b) preclude anyone from inviting beneficiaries to 'opt-in' to the sharing of confidential information for the marketing of goods and services.¹²⁸

This is also in contravention of section 3(c) read with section 16 of the SASSA Act which states that no person may dispose of social grant beneficiary information, unless there is a court order compelling one to

126 Black Sash submission at United Nations General Assembly on Digital Technology, Social Protection and Human Rights in May 2019 9.

127 <https://www.news24.com/fin24/Economy/did-cps-lie-about-its-social-grant-profits-20171119-2> (accessed 20 September 2020).

128 *Black Sash Trust* (n1) para 76.

do so.¹²⁹ Prinsloo contends that SASSA does not have a well-equipped information technology (IT) infrastructure, also imparting data belonging to SASSA beneficiaries to cybercrime syndicates. This effectively means that SASSA is in dire need of an improved IT infrastructure that will not only be beneficial to the agency only but to social grant beneficiaries. Sending misleading information through SMSs to these beneficiaries is said to be an indication of a poor IT infrastructure; staff members are alleged to have sold beneficiaries' confidential information.¹³⁰

The above continued illegal use of data and the infringement of the right to privacy also contravene the provisions of POPIA. The Act is the primary legislation, which was enacted to give rise to section 14 of the Constitution¹³¹ and the principal legislation dealing with data protection and privacy. POPIA is described as serving its envisaged purpose within the data protection spectrum, which is evident through the provision it made pertaining to the development of a comprehensive legal framework.¹³² The Act comprises a chapter dealing with conditions of lawful processing of personal information¹³³ which, among other provisions, provides that information should be collected for a legal purpose¹³⁴ and requires that the concerned party be made aware when collecting information.¹³⁵ The said chapter further contains a crucial provision, which demonstrates proactive steps to be taken as security measures on integrity and confidentiality of personal information.¹³⁶ The responsible party is required to maintain confidentiality and integrity of personal information at its disposal. This is to be done by taking technical, appropriate, reasonable and organisational steps.¹³⁷ This will prevent the 'loss of or damage to or unauthorised destruction of personal information¹³⁸ and unlawful access to or processing of personal information'.¹³⁹ To archive

129 Sec 3(c) read with sec 16 SASSA Act.

130 T Prinsloo & S Ntondini 'The exploitation of South African Social Security Agency grant recipients' data' Proceedings Annual Workshop of the AIS Special Interest Group for ICT in Global Development 2018.

131 Sec 14 Constitution.

132 A Naude & S Papadopoulos 'Data protection in South Africa: The Protection of Personal Information Act 4 of 2013 in light of recent international developments' (2016) 79 *Journal for Contemporary Roman-Dutch Law* 16.

133 Ch 3 POPIA.

134 Sec 13(1) POPIA.

135 Sec 18(1) POPIA.

136 Sec 19 POPIA.

137 Sec 19(1) POPIA.

138 Sec 19(1)(a) POPIA.

139 Sec 19(1)(b) POPIA.

this, the responsible party must take proactive measures that will assist in foreseeing internal and external risks that may be posed to the personal information of the data subject.¹⁴⁰ The responsible party should develop safeguard measures to fulfil this purpose.¹⁴¹ The Act requires responsible parties to continuously do quality checks of the safety system measures to establish whether or not they are still effective.¹⁴² There is no doubt that SASSA's safety net measures have been tampered with on numerous occasions. Thus, they have been rendered ineffective, effectively meaning that SASSA has failed to keep up with its system to enable an effective system that safeguards personal information. To keep abreast with new risks, safeguards need to be regularly updated,¹⁴³ which will allow SASSA to counteract efforts of cybercrime syndicates that explore new ways of accessing grant beneficiaries' personal information and, subsequently, the illegal use of their data and infringing their right to privacy.

Batchelor and Wazvaremhaka note financial illiteracy as another contributing factor relating to the recent invasion of data and privacy. Unfortunately, financial service providers have taken advantage of the fact that most social assistance beneficiaries are illiterate and, as a result hereof, some were exposed to financial discrepancies.¹⁴⁴ Therefore, financial education for social assistance beneficiaries is paramount, which will enable them to better understand how to manage finances. Dutschke reminds us of the primary existence of SASSA, namely, that it was established in order to deal with the poor administration of social grants that existed at the time and this adversely affected the receipt of social grants. The Agency was necessitated by the delay in social grant payments, which was monitored at provincial level, and the establishment of the Agency meant that the responsibility to administer social grant payments will now be transferred to the national level.¹⁴⁵ This was also made possible by the Constitutional Court in the case of *Mashavha v President of the Republic of South Africa* when it declared the administration of social grants to be invalid and unconstitutional but suspended the invalidity.¹⁴⁶

140 Sec 19(2)(a) POPIA.

141 Sec 19(2)(c) POPIA.

142 Sec 19(2)(d) POPIA.

143 Sec 19(2)(d) POPIA.

144 Batchelor and Wazvaremhaka (n 21) 14-15.

145 M Dutschke 'Improving the administration of social assistance services' (2008) 9 *Economic and Social Rights in South Africa* 12.

146 2004 ZACC 6; 2005 (2) SA 476 (CC).

Another factor to be considered that contributes to the illegal use of data and breach of privacy that belongs to social assistance payments is the poor administration at SASSA. There are numerous challenges that affect SASSA to operate optimally. In this chapter all these challenges that have a bearing on the protection of data and privacy that emanate from the Agency are summed up under the term 'poor administration'. For the purposes of this chapter, poor administration includes the delays in payments that are associated with slow capturing, verification and approval, which sometimes is attributed to the fact of shortage of human resources. The absence of technological infrastructure also adds no value in the purpose of archiving effectiveness in the social assistance system.¹⁴⁷ Therefore, it is worth noting from the latter on SASSA's administration that the Agency is grappling with maladministration, which cannot be separated from the shortcomings on data protection and privacy faced by social assistance beneficiaries. In the case of *Cele v The South African Social Security Agency and 22 related cases* the Court expressed its concern over the blockages of applications of social assistance that are occasioned by incompetent officials, poor administration and numerous legal battles.¹⁴⁸

The lack of effective legal measures to protect data and curb efforts to infringe the right to privacy has also been associated with high levels of grant corruption within the Agency. This is evident from the annual report released by the Public Service Commission (PSC), which revealed social grants corruption as the highest corruption, at 2 400 cases between the financial years 2017/2018-2020/2021. Social grant fraud is one of the most reported fraud cases on the national anti-corruption hotline NACH. It is said that most social grant cases are occasioned 'identified along with unethical behaviour, appointment irregularities, service delivery and procurement irregularities'.¹⁴⁹ In the past, due to the high levels of corruption and fraud in social assistance, which included fake identity of receipts and fraudulent claims, this enunciated on SASSA to develop biometrics in a bid to assist in identification and eliminate fraud.¹⁵⁰ SASSA not only is in contravention of POPIA or the SASSA Act by not having effective legal measures, but also contravenes the Social Protection Floors Recommendation 202 of 2012¹⁵¹ as it requires member states to set up

147 http://repository.nwu.ac.za/bitstream/handle/10394/9515/Joseph_DE_Chapter_4.pdf?sequence=5 (accessed 30 October 2022).

148 2008 (7) BCLR 734.

149 <https://citizen.co.za/news/south-africa/investigation/2358392/social-grant-fraud-records-highest-number-of-alleged-corruption-cases-psc-report/> (accessed 2 October 2020).

150 As above.

151 Social Protection Floors Recommendation 202 of 2012.

effective social security systems with proactive steps to protect the data of social grant beneficiaries.¹⁵²

5 Recommendations

With respect to the looming social grants discrepancies, the need to establish the Social Assistance Inspectorate is necessary and urgent as ingrained in chapter 4, section 24 of the Social Assistance Act.¹⁵³ This will enable the inspectorate to effectively investigate and deal with complaints around grant corruption, fraud, the illegal use of data, the infringement of privacy as well as cybercrime of which social grants beneficiaries are victims.

The Social Assistance Act makes provision for the establishment of an inspectorate for social assistance. An executive director must be appointed to head the inspectorate,¹⁵⁴ which will function independently from SASSA and the Department of Social Development.¹⁵⁵ The rationale behind this provision is to ensure the independence of this institution. I hold a different view from the legislature on this aspect, because the envisaged independence of the inspectorate will be impaired and tempted as the Act permits the minister to exercise full responsibility over the inspectorate. In some instances, complaints from social grants beneficiaries may be extended to the minister who can necessitate the inspectorate to also investigate the ministry. The final outcome may be compromised by possible interference, which also affect the credibility of the inspectorate report.

The inspectorate is tasked with maintaining the frameworks and systems of social assistance.¹⁵⁶ It was also tasked to perform internal audits and monitor compliance with the Agency's policy and relevant laws.¹⁵⁷ The inspectorate was also meant to investigate fraud, corruption and mismanagement as well as criminal activities.¹⁵⁸ Since the enactment of the Social Assistance Act, the inception of the inspectorate remains a dream that is not yet realised. South Africa should derive certain lessons from the United States as far as an independent inspectorate is concerned. In the US there has been the establishment of the Office of the Inspector

152 Para 23 Social Protection Floors Recommendation (n 151).

153 Ch 4, sec 24 Social Assistance Act.

154 Sec 24(1) Social Assistance Act.

155 Sec 24(1) Social Assistance Act.

156 Sec 27(1)(a) Social Assistance Act.

157 Sec 27(1)(b) Social Assistance Act.

158 Sec 27(1)(c) Social Assistance Act.

General (OIG).¹⁵⁹ The establishment of the OIG finds expression in the Social Security Independence and Programme Improvements Act¹⁶⁰ and its authority generally emanates from Inspector General Act of 1978.¹⁶¹ The responsibility of the office is to protect social security integrity. The OIG monitors the activities of the management to ensure effectiveness and ensures that it curbs fraud within the social security administration. The inspectorate has been reported to be effective and has assisted in ensuring efficiency as well as eliminating conduct of fraud within social security administration.¹⁶²

Although smart cards were introduced to ensure efficiency with regard to social assistance payments and eliminate possible fraud activities, some obscurities remain as the current method of payment only requires the cardholder or beneficiary to punch in the pin after presenting the card. This can practically mean that anyone can get a hold of the pin and present themselves as the card owner at any pay point or ATM. To curb this detrimental form of payment, card payments that include biometrics payment is hereby proposed.¹⁶³ This method requires a sensor/finger print reader on the card before presenting the card so as to ensure that the individual really is the card holder. Therefore, before the use of the card, the beneficiary will activate their card by using a finger, which will ensure that the card is only used by the owner who is the beneficiary to curb acts of fraud.¹⁶⁴

As highlighted earlier, Net1 and its subsidiaries still possess personal information of social grant beneficiaries, which they use to advertise their products, and they eventually use the data without consent, also infringing their right to privacy. The Constitutional Court judgment in the *Black Sash* case¹⁶⁵ has attempted to curb such malpractice despite the fact that there is no compliance. The Court held that SASSA and CPS must ensure that the following terms and conditions are imbedded in the contact:

159 Social Security Administration (SSA), Office of Inspector General (OIG) Special Agent Handbook, 2002, https://www.governmentattic.org/27docs/SSAoigSpecAgentHdbk_2002.pdf (accessed 27 November 2020).

160 Social Security Independence and Programme Improvements Act of 1994.

161 Inspector-General Act of 1978.

162 Social Security Administration (SSA), Office of Inspector General (OIG) Special Agent Handbook, 2002, https://www.governmentattic.org/27docs/SSAoigSpecAgentHdbk_2002.pdf (accessed 27 November 2020).

163 S Mthethwa & M Thiyanne 'An improved smartcard for the South African Social Security Agency (SASSA)' 3rd International Conference on Information Science and Security, Pattaya, Thailand, 2020 3.

164 As above.

165 *Black Sash Trust* (n 1) para 1.

- (a) contain adequate safeguards to ensure that personal data obtained in the payment process remains private and may not be used for any purpose other than payment of the grants or any other purpose sanctioned by the Minister in terms of section 20(3) and (4) of the Social Assistance Act 13 of 2004;¹⁶⁶ and
- (b) preclude anyone from inviting beneficiaries to 'opt-in' to the sharing of confidential information for the marketing of goods and services.¹⁶⁷

Therefore, the state needs to ensure that there is compliance with the Constitutional Court judgment, and Net1 should return the grant beneficiaries' personal information to SASSA as the chief custodian of personal information of social grant beneficiaries. In the case of failure or refusal by Net1 to hand over the personal information belonging to grant beneficiaries, the state should lodge an application of contempt of court. To further compel Net1 to comply with the provisions of the Constitutional Court judgment and to ensure that the state execute the order effectively and efficiently, one needs to build a substantive argument through the lenses of the ongoing discourse of judicial enforcement of socio-economic rights. The enforcement of socio-economic rights has come under close scrutiny in two famous Constitutional Court cases, namely, the *Grootboom* and *Soobramoney* cases. The significance of these cases on this aspect was thus amplified in the *TAC v Minister of Health* case wherein it reiterated that the state is under a constitutional obligation to comply with or fulfil the obligations imposed by sections 26 and 27 of the Constitution.¹⁶⁸ De Beer and Vettori submit that over the past years the judiciary has been rather creative and cautious in treating matters relating of socio-economic rights with the urgency they deserve. The non-compliance by state officials and other personnel may be regarded as a high level of ignorance and arrogance about their duties as well as the powers of courts of law in this regard. They further submit various modes of enforcing and ensuring compliance with judgments on socio-economic rights such as structural interdicts, contempt of court, as mentioned earlier, and delictual damages.¹⁶⁹

The judicial enforcement of socio-economic rights cannot be overemphasised but rather demonstrates the causal nexus between the said enforcement and data protection and privacy. If there is no adequate protection afforded to social grant beneficiaries in terms of their personal

166 *Black Sash Trust* (n 1) paras 76, 6.1(a).

167 *Black Sash Trust* (n 1) paras 76, 6.1(b).

168 *TAC v Minister of Health* para 23.

169 RJ de Beer & S Vettori 'The enforcement of socio-economic rights' (2007) 10 *Potchefstroom Electronic Journal* 26.

data and privacy rights, this eventually impairs their right to social assistance, which is categorised under the umbrella of socio-economic rights. On account of the latter fraud, corruption and cybercrimes are perpetuated as a result of the state's failure to honour the Constitutional Court judgment, with appalling consequences for the needy and vulnerable social grant beneficiaries. Hence, I concur with De Beer and Vettori on the alternatives they have explored, namely, should the state fail or refuse to execute the judgment, which include structural interdicts, contempt of court and delictual damages.

POPIA¹⁷⁰ gave rise to the establishment of the Information Regulator, which functions in accordance with this Act¹⁷¹ and Promotion of Access to Information Act.¹⁷² The Information Regulator is accountable to the National Assembly.¹⁷³ The state together with SASSA should make use of the Regulator as an enforcement agency in cases of illegal use of data and invasion of the right to privacy. While there is no hope of commitment by the state to establish the social assistance inspectorate, SASSA can in the meantime partner with the Regulator in eliminating all forms of illegal use of data belonging to grant beneficiaries that impairs their right to privacy. Among the duties, powers and functions of the Regulator, the Regulator promotes the lawful processing of personal information¹⁷⁴ and also oversees both private and public institutions' compliance with the provisions of POPIA.¹⁷⁵ Furthermore, the Regulator has the power to receive and investigate complaints pertaining to the misuse of personal information.¹⁷⁶ With such provisions of POPIA that empower the Regulator to decisively deal with acts of impropriation of data and invasion of privacy, SASSA may consider the Regulator a better institution to protect data and privacy rights of grant beneficiaries.

Since the introduction of technological changes in the Agency, there has been resistance from workers, evidenced by the workers' protest led by National Education Health and Allied Workers Union (NEHAWU). Top on the list of demands was that biometric enrolment was impractical given the fact that most SASSA branches are less equipped and most staff are not technologically capacitated, and that they would need to undergo

170 POPIA (n 96).

171 Sec 39(c) POPIA.

172 Promotion of Access to Information Act 2 of 2000.

173 Sec 39(d) POPIA.

174 Sec 40(1)(a)(i) POPIA.

175 Sec 40(1)(b)(i) POPIA.

176 Sec 40(1)(d)(i) POPIA.

training before enrolment.¹⁷⁷ Hence, it is recommended that it would be prudent for the Agency to arrange continued training to enable workers be familiar with the advanced system. This will also ensure the proper running of the Agency without any hiccups relating to maladministration.

Many grant beneficiaries are vulnerable and illiterate people who lack financial capabilities, as highlighted earlier on. SASSA should also focus more on financial education of these social grant beneficiaries to improve their financial capabilities and better handling of their finances. The South African Grant Distribution report highlights some meaningful impacts on these people if financial education is conducted. These factors are the following:

- increase grant recipients' household and personal ability to achieve their medium and long-term financial goals;
- increase their household and personal overall welfare;
- enable grant recipients to build on their increased resilience;
- support the most vulnerable segments to be able to cope with hardships, and avoid falling into food insecurity or deep and sustained misery;
- improve the financial sector's ability to cater for the needs of low-income segments of the market;
- foster South Africa's economic growth;
- ensure that the nation's budget can become more sustainable and ensure that public expenditures are affordable for the nation, thus reducing the debt burden on the economy.¹⁷⁸

6 Conclusion

Social assistance programmes that have been implemented over the past years are evidence that the state is committed to archiving socio-economic rights, because social assistance programmes are based solely on government's revenue in order to effect social grant payments to the needy. Due to the technological advancements in the area of social grants through SASSA, it has thus necessitated the enactment of legal measures to prevent the beneficiaries from being exposed to crimes by and conduct of cyber syndicates. It is against this background that a legislative framework was enacted, but most importantly to give rise to section 14 of the Constitution.

177 <https://www.timeslive.co.za/news/south-africa/2018-10-10-sassa-workers-go-on-strike> (accessed 12 December 2020).

178 South Africa SASSA Grant Distribution Improving the financial capability of grant recipients report, https://www.finmark.org.za/system/documents/files/000/000/276/original/SASSA_Grant_Recipients_-_Improving_the_Financial_Capability.pdf?1605614633 (accessed 15 December 2020).

Social assistance beneficiaries are entitled to social assistance programmes should they be unable to support themselves, as entrenched in section 27 of the Constitution.¹⁷⁹ All that is required from them is to submit their documents with their personal details to the processing officer who later processes the application and the applicant will be informed of the outcome of the application. During this period and even afterwards, the applicants enjoy constitutional protection of their personal information through section 14 of the Constitution.¹⁸⁰ With these constitutional rights bestowed on social grant beneficiaries, the state is constitutionally obliged to respect, protect, promote and fulfil the rights in the Bill of Rights.¹⁸¹ Not only do grant beneficiaries enjoy constitutional protection but legislative protection as well through the lens of section 16 of the SASSA Act,¹⁸² which prohibits anyone from disposing of any information relating to the social grant beneficiaries subject to the provisions of the Constitution, POPIA¹⁸³ or a court order.¹⁸⁴

Therefore, the *Black Sash* case paved the way forward to enable the state to effectively protect social grant beneficiaries' data from illegal use and to avoid the infringement of their rights to privacy. Safeguard measures should be a priority for the state when processing social grant applications. Even after the application process the state is under an obligation to safeguard personal information belonging to social grant beneficiaries.

179 Sec 27 Constitution.

180 Sec 14 Constitution.

181 Sec 7 Constitution.

182 Sec 14 Constitution.

183 POPIA (n 96).

184 Sec 16(1) SASSA Act.

References

- Batchelor, B & Wazvaremhaka, T 'Balancing financial inclusion and data protection in South Africa: *Black Sash Trust v Minister of Social Development* 2017 (9) 1089 (CC)' (2019) 136 *South African Law Journal* 129
- Currie, I & De Waal, J *The Bill of Rights handbook* (2016)
- De Beer, RJ & Vettori, S 'The enforcement of socio-economic rights' (2007) *Potchefstroom Electronic Law Journal* 26
- Dutschke, M 'Improving the administration of social assistance services' (2008) 9 *Economic and Social Rights in South Africa* 12
- Greenleaf, G & Cottier, B 'Comparing African data privacy laws: International, African and regional commitments (2020) 4, <https://citizen.co.za/news/south-africa/investigation/2358392/social-grant-fraud-records-highest-number-of-alleged-corruption-cases-psc-report/> (accessed 2 October 2020)
- Mthethwa, S & Thiyanne, M 'An improved smartcard for the South African Social Security Agency (SASSA)' 2020, 3rd International Conference on Information Science and Security, Pattaya, Thailand 3
- Naude, A & Papadopoulou, S 'Data protection in South Africa: The Protection of Personal Information Act 4 of 2013 in light of recent international developments' (2016) 79 *Journal for Contemporary Roman-Dutch Law* 16
- Orji, UJ *The African Union Convention on Cybersecurity: A Regional Response Towards Cyber Stability?* (2018)
- Peekhaus, W 'South Africa's Promotion of Access to Information Act: An analysis of relevant jurisprudence' (2014) 4 *Journal of Information Policy* 570
- Prinsloo, T & Ntondini, S 'The exploitation of South African Social Security Agency grant recipients' data' (2006) *International Journal of Social Welfare* 16
- Roos, A 'Core principles of data protection law' (2006) 39 *Comparative and International Law Journal of Southern Africa* 103
- Roos, A 'Personal data protection in New Zealand: Lessons for South Africa?' (2008) 11 *Potchefstroom Electronic Law Journal* 90
- Van der Merwe, D *Information and communication technology law* (2016)