No. 5 Louis Raymond Street
PO Box 11618
Windhoek
Fax.: 088620356
eben@isgnamibia.com

23 AUGUST 2021

REPORT ON STATUS OF VARIOUS POLICIES AS CONTAINED IN THE HARAMBEE PROSPERITY PLAN II

Data Protection Bill
Cyber Crime Bill
Land Reform Bill
National Informal Economy & Entrepreneurship Policy and Attendant Bill.

1. Introduction

EPRA's objective is to advocate for pragmatic, sustainable, pro-growth and investment friendly economic policy in Namibia. Since its inception, EPRA made substantial effort to research and provide comment on the National Equitable Economic Empowerment Bill (NEEEB) and the Namibia Investment Promotion Act (NIPA).[1] The original version of NEEEB was published during February 2016 and NIPA was promulgated during August 2016.

Since 2016, Namibia's economy contracted substantially, investment declined to levels last seen before independence, countless businesses closed, and tens of thousands of Namibians lost their jobs. Furthermore, since 2016, Namibia's credit rating was reduced several times by both Moody's and Fitch rating agencies, now standing at the lower end of the "non-investment grade / speculative" bracket, commonly referred to as "junk status". During this time government debt ballooned. ERPA agrees with numerous local and international experts that NEEEB and NIPA substantially contributed to this economic decline.

We continue to keep an eye on emerging policies as the possible devastating consequences of government policy becomes increasingly clear. We believe that we cannot significantly grow our economy while our country continues to pursue economically destructive policies. We further believe that we can cause further, substantial harm to our economy if future policies do not meet the standards expected from a free, constitutional, democratic society supporting the rule of law.

From experience we fear that future policies may be used in a further attempt to create and empower institutions of extraction and corruption, as we have seen with the amendments to the Marines Resources Act and subsequent regulations and gazetted agreements thereto, which directly enabled the "fishrot" corruption scandal. These statutory provisions sailed through Parliament unopposed, condoned, or even unnoticed by opposition parties.

[1] For our publications visit https://www.epra.cc/downloads/

Namibians place substantial trust in the structured legislative system whereby laws are created. A substantial portion of Namibians rely on the oversight opposition parties supposedly provide to curtail the creation and expansion of institutions of extraction. This creates a false sense of security. The use of political power for self-enrichment and means other than to serve the electorate, especially through the legislative process, is now well known as "state capture", following the disastrous looting of public assets by politically deployed cadres in South Africa. Also, from the South African experience, we have witnessed the capture, and outright destruction of institutions that would traditionally be tasked with the protection of public interests and assets and the prosecution of state looters.

Civil society played a significant role in exposing state capture. Some argue that only civil society exposed state capture. What is clear is that, left to their own devices, the ruling ANC party would have never exposed this rot. The ANC continued to deny the existence of this cancerous system and only after public pressure forced the establishment of the Zondo Commission, was a mountain of evidence exposed to conclusively prove that the existence and the magnitude of state capture is now unquestionable.

There is increasing concern that Namibia is following in the footsteps of South Africa's state capture methodologies, especially through the legislative process, and also through the capturing of institutions. For this reason, EPRA resolved to become more active in assessing newly proposed national policies (which include proposed laws and proposed amendments to existing statutes).

In the latest national planning document, the Harambee Prosperity Plan II, Goal One is Accountability and Prosperity, to be achieved, inter alia through an activity which will see the "adoption and enactment of key policies and legislation". These include, inter alia, NEEEB and NIPA. Others include:

- The Data Protection Bill,
- The Cyber Crime Bill,
- The Land Reform Bill,
- The National Informal Economy & Entrepreneurship Policy and Attendant Bill.

In this report EPRA provides a short summary of the status of NEEEB and NIPA. EPRA also researched the status of the above-mentioned four bills and, where available, this report provides an assessment on each. The assessment focuses on constitutionality, possible derogation of the rule of law, and possible adverse effects on the enabling environment needed for investment and private sector growth. Our assessment also takes into account that several experts have in the past warned that state control is becoming a substantial obstacle to investment and economic growth and where appropriate we report on possible unreasonable and/or undesirable expansion of state control through these bills.

2. NEEEB and NIPA

In respect of NEEEB, EPRA provided an extensive report[2] and made submissions to the newly established Namibia Investment Promotion and Development Board (NIPDB). We were

[2] Visit www.epra.cc/downloads/ for a copy of this report.

informed that submissions were assessed by NIPDB, who then made recommendations to the Office of the Prime Minister. As the Government remains unconvinced that NEEEB contributed to Namibia's economic decline since 2016, we are not optimistic that any major positive changes will be made to any newer version of NEEEB. We hope to be proven wrong.

On NIPA: We are informed that, to improve the Act, extensive work was done by an industry committee, in cooperation with Ministry of Industrialisation, Trade and SME Development (MITSMED). We are further informed that NIPDB also appointed consultants to assess NIPA. We do not know if NIPDB's assessment considered improvements previously suggested by the said committee. NIPDB is now in the process of providing its recommendations to MITSMED.

Unfortunately, the policy uncertainty on NEEEB and NIPA remains, and probably will do so for some considerable time.

3. Cybercrime Bill

In this section we provide an assessment of the Cybercrime Bill which we believe (but cannot know for certain) is the latest version.

3.1 Introduction

This bill is very likely unconstitutional, for various reasons. It clearly impugns the constitutional right to privacy. This is acknowledged in the bill itself. It provides for wide-ranging powers to a "Management Committee" (of possibly only two persons) to access any data and communication in private domain, on the sole discretion of the Minister responsible for technology.

There is no specific safeguard of data that would otherwise be confidential, for example information subject to client-attorney privilege, doctor-patient privilege, funding to political parties within the statutory prescribed limits, membership to private institutions, even intellectual property held by private organisations or businesses. The data on ongoing investigations by the Anti-corruption Commission can also be accessed by persons appointed through political channels, and even be shared with foreign entities.

The bill does address some legitimate issues of concern, such as cyber hacking and child pornography, but the powers provided to Government to access private information in the process are largely unlimited. Once Government uses this power to obtain otherwise private data and communications, there is no remedy, for the data would have been accessed and possibly distributed already. A court cannot be approached to interdict the Government from accessing data as the process up to such point of access is done in secret, unknown to any affected person.

There is little safeguard against government surveillance of private citizens and organisations for possible sinister reasons, which then allows for the State to become a surveillance state unchecked by constitutional safeguards. We urge policymakers to revisit this bill and reconsider the issues addressed herein.

1.1. Scope of the Bill

All computer systems and data message fall within the scope of the bill. This will include all storage and transmission of data as well as electronic mail, mobile communications, SMS messages, and video and audio recordings. All servers, personal laptops and mobile phones are regarded as computer systems.

All facilities generating, sending, receiving storing or processing data or data messages fall under this bill.

A person is deemed to personally possess data even if such data is stored by a third party as a service to such person.

3.2 Enforcement

A Computer Security Response Team (Csert) is established within the Communications Regulatory Authority of Namibia (CRAN) to enforce the bill.

The powers of Csert vests in a Management Committee established by CRAN, which Management Committee can consist of as few as two people. The Management Committee has all the powers, functions and duties conferred upon Csert.

Cert may collect "all relevant information" and "monitor" anything relating to the security and stability of computer and information systems. It may disseminate such information in its own discretion to any third party. Csert may also co-ordinate its actions with a foreign "body".

Csert may "take all necessary steps to diminish the risk of offences involving" the uses of computers, including the "detection" of such offences. These offences are extremely broad as discussed hereunder, and thus Csert essentially has *carte blanche* to access private information, in its own discretion. Furthermore, the power to "detect" logically precedes an inference that an offence was committed, thus giving Csert the powers to access any data and communication on any electronic devise without having to show reasonable cause that a crime is being committed. Reasonable belief that a crime is being committed, urgency, and a real risk of destruction of evidence are prerequisites for the police to breach the right to privacy. These will not be requirements under this bill.

In addition to the general powers described above, Csert may take "all reasonable steps" to "detect" money laundering or the "hiding of proceeds of crime" through the use of a computer system. Again, the steps that can be taken to "detect" precedes an inference that such actions took place, thus giving Csert the powers to access any private data or communications based only on the assertion that such actions could possibly have taken place. Apart from these specific powers, Csert may also do anything that is necessary or desirable for the purpose referred to above. Such unlimited powers cannot possibly withstand constitutional muster, as is evident from several prior Supreme Court judgments.[3]

[3] Most notably the Supreme Court Judgments in MAN vs NMRC and Telecom vs CRAN

The bill also makes provision for CRAN's board to delegate "any power or assign any duty or function" to the Management Committee, even if not expressly stated as a power, duty or function of Csert in the bill.

To enforce the bill inspections may be conducted, and "any institution" or "person" may be appointed as "Computer Security Inspector" (CSI), whether employed in Public Service or not. CSIs may conduct inspections on "security, stability or confidentiality" of "important" databases. A CSI, or any person delegated by a CSI, may run a "test" on any "important database" without giving notice, and such test "may involve the access of the system without authorisation" of the official user. A CSI may issue fines.

3.3 Funding of Csert

A Computer Security Fund will be established to defray the expenses of Csert. The fund will be funded through Parliamentary budget, and also "monies paid as a consideration for security services provided by Csert". The bill does not state who will determine such charges, who will be liable to pay such charges, and under what circumstances. Csert may also receive funds "derived from any activity relating to its functions".

From the above it appears that the policymakers wish to enable CRAN to impose levies and otherwise prescribe payments for mandatory services to be provided to certain entities, perhaps even individuals.

3.4 Effective full access to all data and communications

The Minister may declare any data, including communications, as "important data" if in his/her sole discretion it is in the interest of national security, or "the economic or social well-being of Namibia". Once so declared Csert (read Government) obtains substantial control over such data. The Minister may issue regulations on "any matter relating to access to, transfer and control of important databases". The Minister may also state to whom data must be revealed and may prescribe who may audit a database (which audit will be compulsory) as well as the content of an audit report to be provided to Csert.

Non-compliance with the newly formed powers of Csert to access data will be a criminal offence punishable by up to five years imprisonment.

Apart from the fact that there is no Parliamentary oversight on the Minister's discretion to breach the constitutional protection of privacy, it can be argued that almost all data somehow relate to the "economic or social well-being of Namibia". Again, this allows for massive expansion of the surveillance state, with no remedy to affected citizens other than to challenge the constitutionality of the powers given to the State through the bill itself.

It should also be taken into account that Government is openly and actively expanding its encroachment into private sector business, competing against private sector businesses with public funds. Accessing data in the private domain can greatly assist Government in obtaining an even more unfair competitive advantage over private sector. This inevitably leads to the decline of private sector, and the economy.

In illustration of the above: Namcor competes directly with private sector fuel wholesalers and retailers. Namcor is soon to become an active player in the complete fuel supply chain in Namibia. This is done with public funds, paid for by taxpayers and all consumers of fuel. Private sector is thus funding its own demise, and is forced to enable the reduction of the number of taxpayers.

Through this bill Namcor, and other public sector enterprises competing with private sector in all industries, may gain access to information which can provide them with a further advantage in competing with, and ultimately crowding out private sector, ironically under the guise of the "economic or social well-being of Namibia". In this regard the bill appears to be a further step towards a socialist economy (not to be confused with the concept of the welfare state), an economic model which has always failed in other countries in the past. The Government simply runs out of other peoples' money and potential investors flee, as we have witnessed in Namibia over the past five to ten years. It will be no solace to potential investors to know that their data and communications could now also be freely available to Government, and any local or foreign entity which our government may wish to provide it to.

As stated before, the bill makes no provision for protecting privileged / confidential information from being accessed by the Government.

3.5 Obscuring public data

For decades civil society has fought hard for the promulgation of an Access to Information Act. This is a crucial instrument in civil society's fight against especially government corruption, and especially at a time when public trust in official institutions established to fight corruption is waning. Despite being tabled in Parliament on 17 June 2020, the Access to Information Bill is still not promulgated.

The Cybercrime Bill can be used to undo all the progress made on the Access to Information Bill, even if the latter is passed into law. So, for instance, the Minister may restrict access to or transfer of any database (including communications) which in his/her sole discretion is regarded as "important". Furthermore, the Minister may make regulations to "secure confidentiality" of such databases and prescribe the "procedures and technological methods to be used for storage or archiving" thereof as well as the specific information system it must be stored on, which could possibly include the actual location of such storage.

Once the Minister has decided that a database is "important", he/she may also set the exact circumstances under which and to whom such data may or must be disclosed. The Minister may specify classes or categories of persons to which "important" data may not be revealed and who may not have access to an "important" database. In addition to the above the Minister may regulate "any other matter" pertaining to inter alia the confidentiality or control of "important databases".

Non-compliance with the newly formed powers of the Minister to conceal data, i.e. accessing data specified as "important" will be a criminal offence punishable by up to five years imprisonment.

These powers can easily be used, as the bill stands in its current format, to prohibit access to otherwise public information. For example, the Minister could declare the database on allocation of resettlement farms as "important data", and through the powers in this bill limit access thereto and ensure that same remain "confidential" and thus not open to public scrutiny. Same goes for fishing quotas for example, or public tenders.

3.6 Unauthorised Access

Accessing a computer system or information system, performing an action on data, while knowing that such access is unauthorised, is a criminal offence punishable by imprisonment of up to 10 years, and if the intent was to cause "major disruption" or "serious damage" (which terms are not defined and thus completely arbitrary) by up to 20 years.

While the rationale behind this part is understandable, to criminalise data hacking, cybercrime, ransomware etc., the wording of this part also criminalises, on same equivalence, a person accessing his/her spouse's mobile phone, or logging into his/her Facebook or Instagram account, with no malicious intention. Should the spouse become disgruntled with him/her at some point in time thereafter, even years later, for any reason imaginable, perhaps in bitter divorce proceedings, and he/she then decides to institute a criminal complaint, the spouse faces 10 years imprisonment, while having had no intention to cause any damage at the time.

3.7 Electronic Harassment (vs Freedom of Speech)

The part of the bill dealing with electronic harassment criminalises the action of posting (i.e. on Facebook) or sending a data message (i.e. on Whatsapp) which causes "serious emotional distress", "makes a credible threat of violence or other harm" to a person. Similarly, it will be an offence to make a "statement" in such data posting or message knowing it is false, or with "reckless disregard whether it is true or false, with the intention to do serious harm to the reputation of another person". Making a sexual suggestion knowing it to be "offensive or annoying" will also be a criminal offence.

These offences are punishable by a maximum of two years imprisonment.

Although these new offences may at first glance seem appropriate to some, they pose a material threat to the constitutional right to freedom of expression. This is illustrated by a few examples, some posed in question format, hereunder.

If one would publish a comment alluding to the fact that the Inspector General's recent comment on the police taking control of the City of Windhoek's Council is not only undemocratic and flies against the principles of the Constitution but amounts to outright instigation of an authoritarian police state, the Inspector General would be able to have that person arrested and prosecuted under this bill.

If one reposts an article on Facebook, which article is already in public domain, but it later turns out some statements in that article were not true, perhaps even speculative, or at least not properly researched, one commits a crime as, given the description of the crime, one has not shown sufficient regard whether the article is true or not. One thus now has a duty to

conduct a forensic investigation of sorts on the accuracy of every post you receive, before reposting.

If one expresses a personal opinion that you believe a certain Minister is not competent enough to deliver on a given mandate, do you cause "harm" to that Minister, or can the Minister claim that you have offended his reputation? Likely so, and for that reason you have committed a crime and the Minister may institute criminal proceedings against you. This will be the case even if your post spoke to "Government" generally.

If the leader of a political party distributes a newsletter to his followers, telling them that he believes those currently in power are corrupt, and should be replaced, has he injured their reputation, and may he be jailed for such statement under this bill?

If a 20-year-old boy meets a girl whom he really likes and is audacious enough to SMS her to state that he thinks she is a great person and hope to get to know her much better, and perhaps have an intimate relationship with her, should this be punishable by 2 years imprisonment if she is a person who finds such a message "annoying"?

The list is endless.

If a husband wishes to reconcile with his wife during a break-up and sends her a message that he wishes to re-establish their intimate relationship, as they have had during the start of their marriage, and the wife finds this "annoying", should he be held criminally liable for the mere sending of this wishful message?

The prohibitions stated through these offences far outstrip the rational practicality of daily interactions of ordinary citizens in a free and democratic society, apart from the fact that our civil and criminal law already caters for the bulk of the unwanted actions described therein. So, for instance *crimen injuria* (wilful injury of a person's dignity) is already a common law crime. An utterance based on racial discrimination is already a crime. Unlawful defamation is already grounds for compensation. And so forth. Curtailing freedom of expression through the broad descriptions of these offences will make most social media users instant criminals, for mere reporting of already public posts, and will severely curtail any criticism of any person or institution serving in any public interest position. Practically, no social media post can be forwarded without doing, and recording, a diligent fact-checking exercise, which is a duty no law should confer on the general public, apart from the fact that it severely hampers a free-flow of ideas, which is crucial for the advancement of a free, democratic society.

Ultimately, who decides what is true or false, what is harmful, what constitutes reputational damage? By creating these offences, the Namibian police will be policing these value judgments, and in the discretion of the police, a person may be jailed until he/she is brought before a court. This advances a police state as described in George Orwell's book "1984", where citizens speak only in secret, and hide in the shadows, too afraid of the Thought Police. To curtail a whole nation's freedom of expression in order to protect the feelings of others is a dangerous turn towards a totalitarian communist state.

3.8 Extra-territorial effect

Any offence created in the bill is "deemed to have been committed in Namibia … if any part of the offence was performed in Namibia …. or … if the offence was committed by a citizen of Namibia".

To further expand on the adverse implications of the offences created by the bill, and more in particular the offences relating to "electronic harassment" the following real-life practical example is provided:

The now famous Al Jazeera documentary dubbed the *fishrot* scandal first aired in Namibia in late 2019. It was aired on the Al Jazeera channel facilitated by Multichoice Namibia, and was widely distributed on several social media platforms, including Youtube and Facebook.

There can be little doubt that the ministers implicated in that documentary must have felt "harmed" and their reputation damaged. As per their numerous defences in several courts so far, during several bail hearings, they obviously do not agree with the allegations made in that documentary. Famous Namibian lawyer Norman Tjombe also provided his opinion in the documentary, stating that from what he has seen in the documentary, the crime of corruption was committed.

Under the bill in question Al Jazeera, and especially its journalists and management, could be criminally prosecuted (for the documentary aired in Namibia). Facebook and Instagram could be criminally prosecuted, for they control information systems through which the documentary was distributed, and Norman Tjombe could be prosecuted, for it could be argued that his opinion, which led to "harm" the ministers' reputation, did not follow his own, documented investigation into all the facts in the fishrot matter.

3.9 Duty to provide evidence against oneself

A crucial element of the constitutional right to a fair trial is the right not to be forced to incriminate oneself. So, for instance a suspected murderer, who refuses to tell the police where he hid the murder weapon, cannot be criminally liable for such refusal – only for the murder itself. Put differently, there is no duty on an accused person to do the work of the police or to assist them in any way in the investigation or prosecution.

The bill in question changes this, most likely unconstitutionally, when it comes to all the crimes created in the bill. Any person who refuses to provide to the police a computer password or key, fails to render assistance as requested by the police in their investigation, fails to provide data as ordered by court (which is already an offence termed contempt of court) will commit an offence punishable by a maximum of 2 years imprisonment. The order referred to above can be obtained by the police without the court hearing the other party. The duties, and possible criminal sanctions that may follow, thus stem from proceedings to which the affected person had no opportunity to reply to. No relief can be obtained from a court beforehand, as the affected person was not aware of this invasion until it happened.

3.10 Provision of data to foreign authorities

The bill allows for information obtained under it to be provided to foreign "institutions or bodies". So, for instance data constituting crucial intellectual property of a private Namibian company can be provided to a foreign entity or government wanting to compete in the same industry as the Namibian company. As outlandish as this may sound, this threat is real. The Namibian Government notoriously provides major capital projects to companies owned by China. The Namibian public has rightfully questioned the rationale, and possible ulterior motives behind this seemingly standard government practice.

Namibians and the Namibian private sector often suffer for this. An example is the allegations of City of Windhoek partnering with the Chinese tech company Huawei to monopolise the fibre communications space in Windhoek, possibly through corrupt deals with powerful local officials. The matter was reported to the Namibian Police and then ACC last year, but nothing came of it. In the meantime, CRAN itself, the enforcer-to-be of this bill, refused the business plan on which this scheme was based, despite a duty to provide same, as the statutory steps required to keep such plan confidential were not taken.

China is an authoritarian surveillance state by any definition. One wonders what role this bill may play in not only moving Namibia closer to becoming such a surveillance state as well, but perhaps even assisting other surveillance states, for ulterior motives of a few?

3.11 Omnipotent Minister

Apart from the Minister's powers to make far reaching regulations as discussed above, the Minister is given the general powers to regulate "any matter that is reasonably necessary or expedient to be prescribed to achieve the objectives" of the bill. As also stated before, such "catch-all" statutory powers have in the past been declared unconstitutional by the Supreme Court and should not be included in any new legislation.

The reasons forwarded in these several rulings also speak to EPRA's concerns over this bill, unlimited powers, which are by their wideness open for abuse, and uncertainty on what Government may, and will eventually do with them. It is of little comfort if Namibians are assured this will not happen. The question is, <u>can</u> it happen under the bill? Clearly the answer, as the bill currently stands, is an unequivocal "yes".

3.12 Conclusion on Cybercrime Bill

We implore our policymakers to identify the numerous constitutional rights and freedoms (not only the right to privacy as stated in the bill itself) this bill will breach and to then continue to engage civil society, the Namibian public, to amend the bill to ensure that the protection it aims to provide is balanced, reasonable, and achieved through constitutional means while upholding the principles of the rule of law.

4. Data Protection Bill

We are generally satisfied with the aim of this bill, the protection of personal data controlled and processed by third parties. Unfortunately, the protection provided in this bill against abuse by public bodies may largely be nullified by the Cybercrime Bill, as discussed before.

Furthermore, several matters do raise concern, as discussed hereunder.

4.1 Scope

The bill aims to regulate the processing of information relating to individuals to protect the fundamental rights and freedoms of individuals, particularly their right to privacy with respect to the processing of such information. It establishes a Data Protection Authority which oversees the bill and regulates the conduct of data controllers and data processors.

4.2 The impact of the Cybercrime Bill

As much as the data of individuals should be protected, the protection will not be enjoyed should the controller or processor of such data act in exercising a "legal obligation". So, for instance, Csert (as discussed before) could access personal data, and control and process it at will, through the powers obtained under the Cybercrime Bill.

4.3 Other instances where protection will not be applicable

Personal data will not be protected where the following are threatened: national security, defence, public safety, important economic and financial interests of the State. As stated under the section dealing with the Cybercrime Bill, it becomes a slippery slope when the State can access personal / private data, while competing commercially with those whose data has been obtained. This provides an exceptionally unfair advantage to the State in commercial dealings and increases the State's ability to further encroach on private sector business. The exception above, i.e., "economic and financial interest of the State" will allow the State to process personal / private data (after it was obtained through the Cybercrime Bill) in a manner which is prohibited to private sector. The business intelligence available to the State will therefore not be available to private sector.

4.4 Lack of protection against state surveillance of individuals

The bill allows for processing of personal data for national security and defence purposes, subject to "independent and effective review and supervision". The bill does not state who shall be tasked with such review and supervision, and what such review and supervision will entail. There should be clear and express provisions which inter alia prescribe the minimum standards and processes in reviewing and supervising state surveillance. Without such clear provisions, meaningful review and supervision is unlikely to occur, and the current provision provides nothing but false hope of some sort of oversight of the State's surveillance of individuals.

4.5 Transfer of data to foreign countries and entities

The bill prohibits the transfer of personal data to foreign countries and organisations unless certain safeguards for protection of such data abroad are in place. This is commendable, but perhaps impractical given the nature of automated social media platforms such as Facebook, Instagram, Tik Tok and Youtube. Unfortunately, again, the Cybercrime Bill can still be used to transfer personal data to foreign bodies (as explained before) and such transfer will not be protected under this bill.

4.6 Data Protection Authority – independent

A Data Protection Authority (DPA) is created to oversee the bill and to regulate data controllers and processors. Although the bill expressly states that the DPA must operate independently, without taking any external instructions in the execution of its duties, the Management Board of the DPA consists of five persons appointed by Parliament from a list of ten nominees provided by Government. Government is thus fully in control of who gets appointed to manage the DPA. The DPA is therefore not independent at all. Civil society, whose interests the bill aim to protect, have no say in the appointment of the Management Board of the DPA.

4.7 Inspections by the DPA

The DPA has authority to "supervise" processing of data by both public authorities as well as private bodies. In such supervision the DPA may conduct investigations. There is no express limitation on the scope of such investigations, which leaves the power to conduct same open for abuse of personal/private data by the DPA itself. The concern raised in respect of the Cybercrime Bill is repeated in respect of this bill – the bill could allow otherwise unlawful access to personal / private data by government functionaries.

The DPA will also have the power to impose administrative sanctions and monetary fines. Such sanctions and fines are not limited in the bill, with the calculation of a "financial penalty" currently still unqualified, and still to be decided upon by the policymakers.

4.8 Lack of judicial oversight

The DPA has the powers to order a temporary or definitive restriction on the processing of and access to personal data. This power can be exercised without following any due process, and without any form of judicial oversight. It is therefore open for abuse and could potentially be used to frustrate or obstruct private sector businesses competing with government or frustrate or obstruct the operations of civil society organisations.

4.9 More levies and no financial accountability

The DPA will be funded through budget allocation by Parliament, as well as by raising fees payable by data controllers. This will effectively result in a levy payable by data controllers, the quantum of which is not defined.

The DPA shall neither be subject to influence by Government during the initial allocation of funds nor with regard to the manner in which the DPA spends its funds. A further, uncertain provision simply states that the DPA "shall be subject to financial control", without providing any detail on what such control should entail, and who shall be responsible to oversee such control.

It is assumed that the aim of this provision is to bolster the independence of the DPA, but the complete exclusion of oversight of the DPA's finances leaves ample space for abuse. It is proposed that the provision must at least expressly state that the Auditor General shall audit the DAP annually and provide such audit report to Parliament.

4.10 Conclusion on Data Protection Bill

The general aim of the bill is commendable. There are however several matters of concern which we hope the policymakers take into account to curtail possible abuse of, and by the DPA. The fee payable by controllers must be clearly quantifiable in the bill, and the definition of "controller" must be relooked, as it is currently too wide. Due process and judicial oversight must be included in order to curtail the DPA's discretionary powers to investigate, access data, and cease an entity's data processing operations.

5. The National Informal Economy & Entrepreneurship Policy and Attendant Bill

ERPA made enquiries on the status of this bill, and we were informed that it is still in policy development stage, and not in the format of a proposed bill yet. We shall continue to monitor the progress on this new policy.

6. Land Reform Bill

Despite numerous requests the Ministry of Agriculture, Water and Land Reform failed to provide us with a copy of this bill. We have however been informed that the policy is already in bill format, ready to be forwarded to the legal drafters. We shall continue our efforts to obtain a copy.

Prepared by **ISG Risk Services**
On instruction of the **Economic Policy Research Association**