Joint Session of the African School on Internet Governance and the United Nations Internet Governance Forum Parliamentary Track

Abuja, Federal Republic of Nigeria, 18 September 2023

Keynote Address

Adv. Pansy Tlakula

Chairperson, Information Regulator (South Africa)

Data governance, access to information, data protection and data flows. Challenges, trends and opportunities from an African perspective with emphasis on the role of Parliamentarians

1. Introduction

The 4th Industrial Revolution has ushered the exponential rise of the digital economy globally. In the past few years, there has been an incredible growth in new information technologies which process astounding amounts of data. This data can contribute to economic development and growth. Data has therefore become a strategic asset globally.The African Union, in recognition of the importance of data as a strategic asset has adopted the Data Policy Framework. The purpose of this document is, amongst others, to " provide the policy framework to African countries to maximise the benefits of a data driven economy by creating an enabling policy environment for the private and public investments necessary to support data driven value creation and innovation." In this policy framework, the African Union states that " essential to the development of the data economy, is ensuring the establishment of a safe and secure data system based on effective cybersecurity and data protection rules and practises, and ethical codes of conduct for those who set data policy, implement it and those who use data, whether in public or private sectors." In addition to data contributing to economic growth, it is also valuable to researchers, policy makers, NGO's and new IT entrepreneurs. Key to the digital economy, is trans- border data flows. For the Data Policy Framework to achieve the desired outcome, it is imperative for the African Union Commission to move with speed to develop the Cross Border Flows Mechanisms.

The growth in international data flows and new technologies in the past two decades have led to the recognition of the importance of the right to privacy and data protection globally. In recent times, the call to adopt a fundamental rights approach to data protection has been growing. There is undoubtedly a link between the right to privacy and other rights such as the right to human dignity, the right of access to information and freedom of expression. This link requires that the right to privacy must always be balanced against the right of access to information.

Many countries globally have adopted data protection laws. In Europe, the General Data Protection Regulation (GDPR) was adopted in 2016 to replace the 1995 Data Protection Directives . The GDPR is legally binding to all member states of the European Union and is undoubtedly the strongest privacy law globally. On the African continent, the African Union adopted the Convention on Cybersecurity and Data Protection (Malabo Convention) in June 2014. It is interesting to note that the AU adopted the Convention despite the fact that the right to privacy, which is the legal basis for data protection, is not mentioned in the African Charter on Human and Peoples Rights. The Convention came into effect in June 2023, exactly 9 years after its adoption after Mauritania became the 15th country to ratify it. 40 countries are yet to ratify the Convention. There have been significant technological advancement such as generative Artificial Intelligence and Chat GPT since the Malabo Convention was adopted in 2014. It is not surprising that the African Union has adopted the Data Policy Framework to bring Africa up to speed with technological advancements that have taken place recently.

The difference between the GDPR and the Malabo Convention is that the former is legally binding and none compliance results in the payment of a hefty fine. The Malabo Convention only becomes binding in countries that have ratified it, and only after it has been domesticated. It is encouraging though that despite its low ratification rate, 35 out of 55 countries have adopted data protection laws and 3 have draft laws. Most countries that have adopted data protection laws have established oversight bodies. As I have already mentioned, it is imperative for the right to privacy to be balanced against the rights of access to information to ensure that privacy is not used to stifle the free flow of information, which is necessary to promote transparency and good governance. It is for this reason that it is important for these rights to be given equal attention and treatment. 27 out of 55 countries have adopted access to information laws and 17 have draft laws. However, the challenge on the continent and globally, is that very few countries have oversight bodies that are responsible for both the right of access to information and data protection. On the continent, only Morocco and South Africa have one oversight body responsible for both. Globally, the United Kingdom, Mexico and Germany are amongst the few countries that have one oversight body responsible for both rights.

On the continent, we have established the Network of African Data Protection Authorities and the African Network of Information Commissioners. These networks can play an important role in advancing data protection and access to information respectively on the Continent. They can do so through the adoption of standard setting documents such as adequacy requirements for trans-border flows of personal data.

The question is, what role can Parliaments play in strengthening data protection and the right of access to information. One of the main responsibilities of Parliament is to hold the executive accountable by ensuring amongst others, that the executive begins the process of ratifying international and regional instruments and domesticate them. If Parliaments on the continent executed this responsibility effectively, it probably would not have taken nine years for the Malabo Convention to come into effect.

As I have already indicated, the digital economy is data driven. Society is increasingly operating on line and this raises concerns about global on line platforms and their control of personal data. On the other hand, digital platforms hold valuable data which can be used to contribute to development objectives such as health intervention or public planning. Hence there is a growing movement globally for digital platforms to make the data they hold accessible. As we all know, disinformation, misinformation and fake news online are the biggest threats to democracy, particularly as far as elections are concerned. One of the ways of addressing this phenomenon is by digital platforms making information accessible to researchers who monitor misinformation on line regarding their policies, research and budget for addressing disinformation and misinformation. The fact check process these platforms employ has not yielded desired outcomes.

To address the contemporary challenges we are faced with, Parliaments must ensure that strong data protection and access to information laws with effective enforcement mechanisms are adopted. The access to information laws must apply to both private and public bodies, including political parties, and must apply to information on line and off line. The laws must establish independent oversight bodies which, preferably should be responsible for both data protection and access to information. This will address the challenges of establishing several bodies that are poorly funded. The oversight bodies must be accountable to the legislature and must have effective enforcement powers. In some of our countries, data protection authorities are located within the ministries of information and communications technology. This is a challenges from the independence point of view. Because of the proliferation of personal data on line, most countries are experiencing serious data breaches. In my country, the data protection legislation requires that public and private bodies that have suffered a data breach must inform my organisation, the Information Regulator, which is responsible for both access to information and data protection. Since the beginning of last year to date, we have received more than 600 notifications of data breaches. Parliaments should exercise oversight on this aspect.

Working in silos will not assist us to deal with the modern day challenges brought about by technological advancements. Multi agency collaboration is imperative. Civil society organisations

also have an important role to play. In my country, civil society has partnered with the Electoral Commission to address disinformation on line in collaboration with a number of digital platforms.Data protection authorities must work with Competition Commissions, Consumer Protection Commissions and bodies responsible for Cyber security where they exist. Several Parliamentary committees such as Justice, ICT and Police must work together in the performance of their oversight responsibilities. Parliaments must be bold enough and summon digital platforms to appear before them to account for disinformation and misinformation on their platforms. We are facing a new frontier in the area of human rights brought about by the advancement in technology and it cannot be business as usual.

I thank you for your attention.