Brief - Digital Rights in Africa

Overview

COVID-19 has increased surveillance and intimate data sharing in precautions and contact tracing efforts. Whether for securing permission to travel or accessing essential services, citizens share their details without certainty of security of data or legal justification (Digital Cooperation, 2019). This is no different to many other instances where citizens provide information for health care, opening bank accounts, opening a social media account or transacting. There is no guarantee that signed consent or affirmative action to one's data would result it that consent being respected or not misused. Data is used for information we consume and share. In some instances, it can be prejudicial or irrelevant in respect of algorithms used. These algorithms create a virtual profile of our preferences, behaviour and even movement (Szoszkiewicz, 2020). This is acceptable in a data-driven society despite the threats of phishing, fraud and other criminal activity (Goldstein, et al., 2018).

The AU plans to strengthen intra-African connectivity through policies and strategies for infrastructure. Information and cyber security. Some progress has been made in 48 member states: resulting in 22,000 students graduating, 770 annual tele-medicine consultations and 6,700 continuous medical education (CME) sessions for health practitioners by September 2019 (African Union, 2020).

Africa's development incorporates emerging technology. Thus, cyber security is a priority – as reflected in the AU's Convention on Cyber Security and Personal Data Protection. Although focus is on data protection and online safety, there are shortcomings in homogeneous policies. Social media taxes, online driven human trafficking, online fraud, censorship, social media block outs, misaligned online permissions frameworks and infrastructural standards reflect much needed work is yet to be impactful. Notable events include the launch of data protection guidelines in May 2018, the first regional forum on Cybercrime in October 2018 and the establishment of a regional cyber security expert group (Internet Governance for Libraries, 2017).

Common violations of digital rights

1. Profiling of Marginalized Groups.

Law enforcement, populist groups and criminal organisations target ethnic minority, gender, and youth groups. Marginalised groups are considered easy targets (Media Legal Defence Initiative, 2015).

2. Search and Seizure of Digital Property

Governments and militant organizations utilize internet censorship to shape the public beliefs and curb dissent. Bloggers, activists, and political opponents are harassed and silenced. Mobile phones are easy targets in times of unrest, curtailing movement actions under auspices of states of emergency or internet security.

3. Censorship

Online platforms have increased the flow of information. Reports of human rights injustice and citizen action widen reach and attention. This can lead to repercussions and reprisals. Private sector and/or telecommunications companies play a role in censorship and independent oversight is needed (Orrell, 2015).

Although there have been negative developments, the right to privacy is still championed. Multilateral cooperation on strengthening privacy controls is increasing (UNICEF, 2017). For example, the European Union adopted the General Data Protection Regulation (GDPR); safeguarding user ownership, or revoking where needed, of their data (Akademie, 2016). Although governments can be perpetrators, they have a responsibility to protect digital rights. This is critical to ensure that rapid advancements in technology respect human rights (Mičunović, 2020).

CONCLUSION

The role of multinationals in ensuring homogenous application of data protection, consent and use should be investigated. African governments should strengthen capacity of infrastructural, security and rights skills across board. From developers, software engineers, bandwidth networks, regulations to financial systems. The rapid increase in innovation and global connectedness need resourcing and action, not just political will. Civil society actors should strengthen work in protecting and mitigating human rights violations facilitated, enabled or strengthened by digital uptake.

References

African Union, 2020. *silencing the guns: creating a conducive conditions for Africas development,* s.l.: s.n.

Digital Cooperation, 2019. *The age of digital interdependence,* s.l.: s.n.

Internet Governance for Libraries, 2017. *A Guide to the Policies and Processes behind the Internet and their Impact,* s.l.: s.n.

Media Legal Defence Initiative, 2015. *Training Manual on digital and freedom of expression online,* s.l.: s.n.

Akademie, D., 2016. *Media Development Guidebook Internet Governance: Media freedom in a connected world,* s.l.: s.n.

Goldstein, D. K., Tov, D. O. S. & Prazeres, D., 2018. *The Right to Privacy in the Digital Age,* s.l.: s.n.

Mičunović, M., 2020. *Author's rights in the digital age: how Internet and peer-to-peer file sharing technology shape the perception of copyrights and copywrongs,* s.l.: s.n.

Orrell, T., 2015. *The African Declaration On Internet Rights And Freedoms:A Positive Agenda For Human Rights Online,* s.l.: s.n.

Szoszkiewicz, Ł., 2020. *Internet Access as a New Human Right? State of the Art on the Threshold of 2020,* s.l.: s.n.

UNICEF, 2017. *Access to the internet and digital literacy,* s.l.: s.n.