Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online): 0493-2137
E-Publication: Online Open Access
Vol:55 Issue:08:2022
DOI 10.17605/OSF.IO/3CA4F

E-GOVERNANCE AND PRIVACY: A LEGAL PERSPECTIVE ON BOTSWANA DURING PUBLIC HEALTH EMERGENCIES OF INTERNATIONAL CONCERN (PHEIC)

NEDNAH KEMUNTO MARAGA

Department of Law and Para-Legal studies, Ba Isago University, Botswana.
Email: nednah.maraga@baisago.ac.bw

SHAKEROD MUNUHWA

Department of Business Management, Ba Isago University, Botswana.

PERVIA KUDAKWENYU NGWENYA

Department of Law and Para-Legal studies, Ba Isago University, Botswana.

DAVID CHIKWERE

Department of Business Management, Ba Isago University, Botswana.

ABSTRACT

Governments with a view of mitigating the Public Health Emergencies of International Concern (PHEIC) occasioned by coronavirus disease 2019 (COVID-19), took disparate interventions to aid the health, social and economic well-being of their economies. The interventions included but were not limited to resorting to e-governance for improvement of service delivery, increase integration of Information and Communication Technologies (ICTs) and to support rapid data collection, reporting, contact tracing and data management in an effort to curb COVID-19 Pandemic. ICTs contribution in the PHEIC have brought about enormous risks to privacy and ultimately infringing on various consumer rights. Consequently, this paper examines the place of e-governance and the right to privacy within the status of COVID-19 Pandemic in Botswana. It considers the nature of risks and vulnerabilities brought about by e-governance from a modernist theoretical perspective. The article aims at analyzing the legislative framework surrounding the data protection and the right to privacy and implications of e-governance on Botswana's society by focusing on the risk with which their human right to privacy is exposed to. The study reveals that e-governance is at the center and pivotal in the digital transformation of the country to the Fourth Industrial Revolution (4IR) but the implementation of various e-governance initiatives requires users to provide personal information without clear guidelines and safeguards. The Data protection Act, 2018 as the main legislative framework ensuring stringent protection of personal data and privacy of data subjects alongside others is not yet fully operational due to the absence of a robust institutional framework. Recommendations are made on how to mitigate the challenges and risks with an emphasis on striking a balance between the protection of public health rights and individual rights.

Key words: E-Governance, Public Health, Covid-19, ICT, Fourth Industrial Revolution

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online): 0493-2137
E-Publication: Online Open Access
Vol:55 Issue:08:2022
DOI 10.17605/OSF.IO/3CA4F

1.1 INTRODUCTION

The world has been under siege due to a Public Health Emergency of International Concern (PHEIC) occasioned by the Coronavirus disease 2019 (COVID-19), that plugged the world end of 2019 and early 2020. The public health crisis is not the first but is definitely unprecedented. Governments with an effort of containing the disease and a view of mitigating the pandemic and its myriad sporadic effects took drastic and disparate interventions (Milne and Costa, 2020) to aid the health, social and economic well-being of their economies. Most Countries in sub-Saharan Africa embraced use of various ICTs in governance (e-governance) to improve service delivery, increase integration of ICT use in governance and to fill gaps in various sectors and to support rapid data collection, reporting, contact tracing, and data management- in an effort to curb the COVID-19 pandemic. This paper examines the place of e-governance from the technical challenges part with regards to security and privacy issues. The context of the human right to privacy within the status of COVID-19 Pandemic in Botswana is explored with regards to the breaches to the rights of the users. It considers the nature of risks and vulnerabilities brought about by e-governance from a modern theoretical and legal perspective and analyses the implications of e-governance on Botswana's society by focusing on the risk with which their right to privacy is exposed to. Thereafter, the paper recommends the strategies and measures that can be employed to mitigate the challenges emphasizing on a balance between the protection of public health rights and individual rights such as the right to privacy.

1.2 BACKGROUND OF THE STUDY

The Government of Botswana through the Emergency Powers Act (Cap.22.04), published the Emergency Powers (Covid-19) Regulations, 2020 aimed at containing the spread of the COVID-19 and ultimately protecting the public health and safety. The regulations included but not limited to; the closure of non-essential services, tightening border controls, imposing restrictions and bans on local and international travel, enforcing curfews and lockdowns and resorting to e-governance and use of various Information Communication Technologies (ICTs) in an effort to curb and minimize the spread of the disease as well ensure continuation in service delivery.

The use of digitally driven ICTs increased rapidly and became a necessary need in society to help mitigate the new normal situations. Sohrabi et.al (2020) note that these measures were in tandem with strategies of active surveillance, early detention, case management and contact tracing. Individuals resorted to the use of various existing digital and frontier technologies especially those on video-conferencing (Maalsen and Dowling, 2020) while most governments deployed existing and novel ICTs for e-governance and contact tracing (Ferretti et.al (2020). This proved to be contrary to the norm on ICTs and e-

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online): 0493-2137
E-Publication: Online Open Access
Vol:55 Issue:08:2022
DOI 10.17605/OSF.IO/3CA4F

governance use in the public sector being a complex phenomenon and unsustainable (Larsson and Grönlund, 2016).

The Government of Botswana was not left behind as the use of e-governance became an integral facet for development, dissemination of information, delivery of services and COVID-19 contact tracing. The initiatives which involved computerizing government services included e-administration, e-education, e-judiciary, e-commerce and e-health, as the forms of e-interactions between government to government (G2G) - within and across the government, government to citizens (G2C), and government to businesses (G2B). The various uses of ICTs in Botswana amidst the pandemic included; digital surveillance, electronic commerce, education continuity (e-learning platforms), telemedicine conferencing (diagnosis and treatment), movement regulation (permit applications) and Crisis intervention through the use of Artificial Intelligence, biometrics, facial recognition data, geo-location data, mobile applications (BSAFE APP), COVID-19 Surveillance and Response Tracker in DHIS2 for contact tracing.

The Botswana Communication Regulatory Authority (BOCRA) Annual Report 2019 shows that Botswana ranks among the top five countries in Sub-Saharan Africa in terms of the International Telecommunication Union (ITU) ICT Development Index, while BOCRA Annual Report 2021 further indicates that the most significant growth was in the Fixed Broadband Internet market. This denotes the importance of Botswana government opting for e-governance during the pandemic as it strives towards transitioning Botswana into a digital economy as we approach the fourth Industrial revolution (4IR).

1.3 STATEMENT OF THE PROBLEM

The use of e-governance in PHEIC such as COVID-19 brings about opportunities for reducing the disaster risks but it equally comes with it various technical, organizational and economic challenges. The accelerated ICTs use raises concerns on their impact on privacy and data protection as it brings about challenges and enormous risks to privacy- a fundamental human right. The digital technologies are data-intensive as they generate a lot of personal biometric and location data thus putting ones privacy and data protection in jeopardy (Klar and Lanzerath, 2020) as no clear guidelines on the use and processing of such information exists. The new reality on increased ICTs use puts consumers in an unusual situation as they are solely responsible for their data privacy protections, or lack thereof especially with the rushed deployment of ICTs to curb COVID-19 and mitigate on its effects. Unlike many other rights, in a data-based world where use of artificial intelligence, various digital technologies and machine learning is thriving, individuals' data privacy or lack thereof has long-term irreversible effect beyond the period of the pandemic (Frith and Saker, 2020). Madianou (2020) highlights that risks posed by digital technologies could result to a second-order disaster. The risks include but are not limited to expose Application Programming Interface ("API") Attacks, Botnet Attacks, and Phishing attacks .and hacker attacks.

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online): 0493-2137
E-Publication: Online Open Access
Vol:55 Issue:08:2022
DOI 10.17605/OSF.IO/3CA4F

With the evolving of COVID-19, collection and processing of accurate data and having a sustainable response on COVID-19 is vital thus need for reliance on digital surveillance data collection mechanisms such as the COVID-19 Surveillance and Response Tracker. **Public health surveillance - a form of digital surveillance(Abad et.al, 2014)** has been **one of the e-initiatives by governments during PHEIC such as Ebola (Wesolowski et.al, 2014) and COVID-19 to identify an outbreak, mitigate the spread, identify, monitor and target interventions (Sekalala et.al ,2020).** Governments are rushing to expand their use of surveillance technologies to track individuals and even entire populations using data such as location/GPS, cell phone, personal or demographical identifiable data etc. to gather location data and track people's movements and whereabouts in response to the COVID-19 pandemic. This measure raises questions and risks on privacy concerns as the personal data and information might fall in the hands of wrong persons, shared and used for other ill purposes. If left unchecked and scrutinized, the challenge of responsible data through this measure has the potential to fundamentally alter the future of privacy and other human rights. This brings about concerns on the balance between individual and collective rights with the right to privacy on one hand and the right to public health on the other.

1.4 RESEARCH QUESTIONS

1. What is the place of e-governance and the right to privacy in Botswana?
2. What are the implications of e-governance on Botswana's society by focusing on the risk with which their right to privacy is exposed to?
3. How effective is the legislative framework of the right to privacy and data protection in Botswana?
4. What are the strategies that can be put in place regarding e-governance and the right to privacy in future PHEIC?

1.5 RESEARCH OBJECTIVES

1. To establish the place of e-governance and the right to privacy in Botswana.
2. To ascertain the implications of e-governance on Botswana's' society focusing on the risk with which the right to privacy is exposed to.
3. To analyse and review the effectiveness of the legislative framework of the right to privacy and data protection in Botswana.
4. To recommend strategies that can be put in place regarding e-governance and the right to privacy in future PHEIC.

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online): 0493-2137
E-Publication: Online Open Access
Vol:55 Issue:08:2022
DOI 10.17605/OSF.IO/3CA4F

1.6 LITERATURE REVIEW

1.6.1 THE RIGHT TO PRIVACY

Privacy, like most things has been affected by COVID-19. Privacy which includes data protection and obscurity (Rengel, 2014) in the cyber space is a common tenet of democratic societies (Gwagwa and Wilton, 2014) as it is a fundamental human right which is internationally recognized and constitutionally entrenched in almost every constitution in the world. Privacy as a right should be protected and promoted to safeguard personal dignity as it is inherent in our nature as humans and the need for its protection goes deeper than merely protecting personal information. It is equally significant in forging relationships with others, preventing discrimination and preserving oneself. The right embodies the presumption that individuals enjoy elements of self-determination and liberty over their personal information and space. This is premised on the position that the right to privacy embodies an area of autonomous development and interaction.

The Constitution of the Republic of Botswana guarantees the right to privacy in Section 9 and provides that no person shall be subjected to the search of his person or his property or the entry by others on his premises except with his own consent or as per exceptions stipulated by law. Makulilo (2018) states that, though constitutionally enshrined and recognized in many African countries constitutions, privacy in the digital era is stated to be just but a fallacy as the concept of privacy is purely theoretical and not practical.

International law recognizes the right as encompassing an important aspect of human dignity which has a personal value intrinsically beneficial to preserving an individual's sense of self- an essential value for society. The right is enshrined in various international human rights treaties such as; Article 12 of the Universal Declaration of Human Rights (UDHR); Article 17 of the UN International Covenant on Civil and Political Rights (ICCPR); Article 11 of the UN International Convention on the Elimination of All Forms of Racial Discrimination; Article 16 of the Convention on the Rights of the Child (CRC) and Article 19 of the African Charter on the Rights and Welfare of the Child. This denotes that the right has risen to an international law level under customary international law. The UN General Assembly through the adoption of Resolution 68/167 in December 2013 affirmed that individuals online or in a cyber space have the same rights as the individual's offline and as such should be accorded similar respect, promotion and protection of the right to privacy in digital communications. The United States (US) Supreme Court in Riley v. California 573 U.S., (2014) noted that ICTs such as mobile phones which are popularly and widely used, involve substantial privacy interests due to their capacity such as having GPS instruments and internet surfing functions which may reveal more information about a data subjects private interests and information, concerns and personal data stored in the devices as well as locations. The European Court of Justice in the Google Spain case further elevated the right to privacy by including the protection of personal data. This is

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online): 0493-2137
E-Publication: Online Open Access
Vol:55 Issue:08:2022
DOI 10.17605/OSF.IO/3CA4F

by regulating search engines such as Google against unlawful access and processing of European Union Citizens personal data without their will.

It is however, not an absolute right as it is subject to limitations and derogations like other rights such as the human right to freedom of expression, freedom of movement and freedom of assembly and association. Such derogations may only be of temporary nature and are allowed when reasonably required for the purpose of protecting the rights or freedoms of other persons in the interests of the public and defense of the country. Any activities that restrict or limit the right to privacy, can only be justified when they are prescribed by law, necessary to achieve a legitimate aim, and proportionate to the aim pursued. The limitation further requires the application of principles of necessity and proportionality. A state of emergency such as the one declared by Botswana is one example that can result to the right to privacy being derogated from during crisis.

1.6.2 PROTECTION OF PRIVACY IN BOTSWANA

The Constitution of Botswana in section 9(1) guarantees citizens the right to privacy of the person, his or her home and other property- a fundamental right though not absolute. In light of the constitutional provision, limitations to the right can only be possible when subject only to the limitations stipulated in the constitution for the protection of public interest, and they should be narrowly and strictly interpreted (Balule and Otlhogile, 2016). The limitation of a fundamental right should adhere to the three-pronged test of legality, necessity and proportionality taking into consideration the data privacy principles of transparency, accountability, information quality, security and data subject participation. This denotes that the government's power to limit the right by collecting personal information for purposes of contact tracing must be considered against its constitutional obligations. If the government through its various institutions such as the security and law enforcement agencies engages in any form of surveillance, it should be constitutional, lawful, proportionate, for a specific and legitimate purpose and within a reasonable time.

Access to the courts is a safeguard against violation of individual's right as all persons are equal before the law. In the case of Ketlhaotswe and others v. Debswana Diamond Company (Pty) Ltd, the High Court was faced with a question of ascertaining whether the constitutionally guaranteed right to privacy protects citizens comprehensively as guaranteed under international human rights treaties or is it only limited to the constitutional provisions. The High court in line with the Court of Appeal in the case of Attorney General of Botswana v Dow [1992] BLR 119 (CA) stated that interpretation of constitutional provisions of human rights and fundamental freedoms by the courts should be done using a broad, generous and purposive approach. The court further held that because the constitution only guarantees the right to privacy of the person, international law should be invoked by the municipal courts as a guide to bridge the gaps present due to the dualist system of application of international law in Botswana. This is premised on the position that dualism disallows direct and automatic application of international law in municipal courts unless incorporated by the legislature. The government has the duty to

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online): 0493-2137
E-Publication: Online Open Access
Vol:55 Issue:08:2022
DOI 10.17605/OSF.IO/3CA4F

protect, promote and fulfil the right and guarantee against its abuse or infringement and domestic laws interpretation must not to be in breach with International law- Dow v. AG [1992] BLR 119 (CA). COVID-19 health data which qualifies as an individual's personal information should be safeguarded when it is collected, processed and stored. Processing of such data should be done in a manner that promotes and protects an individual's privacy. It should be processed in limited circumstances and even then, should never be processed unless sufficient guarantees are provided for to ensure that the processing does not adversely affect the privacy of the subject. Botswana relies on ethical data management guidelines issued by international bodies protecting people's privacy during the pandemic. Its contact tracing processes and procedures are guided by the WHO interim guidance regulations. The COVID-19 Guidelines on contact tracing provide for confidentiality of personal information to protect a patient's privacy. It notes that, contacts are only informed that they may have been exposed to a patient with COVID-19 infection but not the identity of the patient who may have exposed them.

1.6.3 POLICY AND LEGISLATIVE FRAMEWORK OF PRIVACY IN BOTSWANA

Botswana is a signatory to the UDHR and has ratified the ICCPR and the ACHPR. Article 17 of the ICCPR, which reinforces Article 12 of the UDHR, provides that "no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honor and reputation". Further to this, the Human Rights Committee General Comment 16 on the Interpretation of Article 17 of the ICCPR and General Comment 31 on the nature of the general legal obligation imposed on State Parties, show the obligations of Botswana as a state party and duty bearer. The obligation is positive and relates to adoption of policy, legislative and other measures surrounding the issues of privacy and access to information to give effect to the right to privacy both online and offline. The Government of Botswana has enacted various legislations which provide for the protection of the right to privacy. They include; The Data Protection Act, 2018, The Electronic Communications and Transactions Act [Act 14 of 2014], The Electronic (Evidence) Records Act, among others.

The Data Protection Act, 2018,

The Data Protection Act (DPA) is the main regulator for data protection ensuring stringent protection of personal data and regulation of the processing of personal information. It gives effect to section 9 of the Constitution by creating a national legal framework for data protection as it seeks to regulate the protection of personal data and to ensure that the privacy of individuals in relation to personal data is maintained.

To achieve this objective, the Act establishes the Information and Data Protection Commission (sec 4) as a public office with the sole mandate of enforcing the Act. The Act sets out criteria for lawful processing of data, and prevents processing of sensitive data (including genetic and biometric data), with exceptions. In terms of the DPA, personal data processed by the data controller for historical, statistical or scientific purposes should

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online): 0493-2137
E-Publication: Online Open Access
Vol:55 Issue:08:2022
DOI 10.17605/OSF.IO/3CA4F

be done fairly and lawfully and with the knowledge or consent of the data subject in writing. The data collection is for specific, explicitly stated and legitimate reasons and they should be protected by reasonable security safeguards against risks such as loss, unauthorized access, destruction, use, modification or disclosure. With regards to sensitive personal data, the Act prohibits processing it unless consent of the data subject is sought the data subject made the data public, the data is for national security, authorized by written law, for legal purposes, research, statistics or health purposes. The data subject rights are limited largely to access and correction and thus data controller obligations include but are not limited to data breach notification to the Commission and notification to the Commission of automated processing operations.

The DPA creates offenses for contravention of the provisions and stipulates that, a data subject has the right to institute an action for damages in the courts for any contravention regarding data processing. Any complaint alleging interference with the protection of personal data is to be made in writing to the commissioner and the information and data protection appeals tribunal will be able to adjudicate over matters involving the breach of any provisions of the Act. Transfers of personal data to other countries are prohibited, unless to a country on a white-list made by Ministerial Order, or to a country which the Commissioner has determined provides 'an adequate level of protection'.

It is worth noting that with adequate legislation and ineffective enforcement and implementation, the right to privacy will be in jeopardy as the lack of effective oversight and enforcement is bound to contribute to a lack of accountability for arbitrary or unlawful intrusions on the right.

The Cybercrime and Computer related Crimes Act, 2018

To address cyber risks and crimes regionally, the African Union adopted the African Union's Convention on Cyber Security and Personal Data Protection in July, 2014. At a sub-regional level, SADC member states adopted the SADC Model Law on Cybercrime and Computer crime in 2012 modeled on the Budapest convention to guide and facilitate the harmonization of domestic laws on cybercrime, eliminate cybercrime safe havens towards effective international cooperation and further encouraged members to enact domestic legislations (Bande, 2018).

Botswana's parliament enacted the Cybercrime and Computer related Crimes Act (CCRCA) in 2018, to combat cyber and computer related crimes, to repress criminal activities perpetrated through computer systems and to facilitate the collection of electronic evidence. The CCRCA as the domestic legal framework on cybercrime criminalizes cybercrimes which include cyber COVID-19 crimes and stipulates various offences in relation to that. The Act incorporates the minimum requirements prescribed by the Budapest Convention relating to offences against the confidentiality, integrity and availability of computer systems and data. With regards to protecting the right to privacy of an individual, offences breaching confidentiality, integrity and availability

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online): 0493-2137
E-Publication: Online Open Access
Vol:55 Issue:08:2022
DOI 10.17605/OSF.IO/3CA4F

of computer data and systems are created. The offences are with regards to; unauthorized access to computer service, unauthorized disclosure of a password and access with intent to commit an offence.

1.6.4 IMPLICATIONS OF E-GOVERNANCE AND RIGHT TO PRIVACY

The advancement of technology through ICTs and the incorporation of e-governance in day to day activities have necessitated an increase in the risks exposed to the right to privacy in the digital sphere. The implications of e-governance on the right to privacy have both been positive and negative. Positively, it has brought about a paradigm shift for effective, expedient and efficient public service delivery from the traditional approaches (Nkwe, 2012). For instance, it has promoted business continuity and also the COVID-19 tracking system has the advantage of generating individual longitudinal data that can improve reporting of key COVID-19 indicators.

On the negative aspect, e-governance has brought about vulnerability and exposure of data subjects to various other risks. These risks include but are not limited to a lack of public trust in e-governance due to the aforementioned vulnerability. Rushed adoption and deployment of technologies and innovations to curb the pandemic have resulted in disaster capitalism as governments rushed without fully considering the vast risks associated with them (Newlands et.al, 2020). It has highlighted weaknesses in disaster preparedness in relation to force majeure' or dealing with PHEICs and other national and global catastrophes.

2.1 METHODOLOGY

The current study was based on a mixed research methodology that included documents, case studies, and legislative analysis. In order to get significance and empirical knowledge of e-governance and privacy being examined, document analysis necessitated repeated inspection, examination, and interpretation of the data. More specifically, case study analysis was used in practical research with the primary goal of determining how specified legal provisions or legal institutions are applied. The analytical method produced an analysis of documents that summarizes case law and emphasizes trends and issues. Finally, the case study analysis included a review of applicable legislation from various regulatory agencies as well as a review of relevant reports. The nest section looks at the study findings and conclusion.

3.1 FINDINGS AND CONCLUSION

The global spread of COVID-19 shows that governments are willing and ready to implement extraordinary measures which may or may not directly affect the rights and freedoms of the citizenry, to curb a menace. E-governance is at the center of COVID-19 & pivotal in the digital transformation of the country in line with the public sector reform as

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online): 0493-2137
E-Publication: Online Open Access
Vol:55 Issue:08:2022
DOI 10.17605/OSF.IO/3CA4F

we approach 4IR. E-governance through various technological products' promotes and provides more benefits where constitutional and legal underpinnings are promoted openly and democratically. The impact of COVID-19 on the right to privacy is that it has increased the rapid use of ICTs which have in tandem accelerated the risks to informational privacy due to the increase in data creation, collection and processing. The policy and legislative framework of privacy and data protection in Botswana is merely in paper but not operational/functional. This is premised on the position that there is absence of robust institutional framework on data protection (The Information and Data Protection Commission which is the regulator/regulating authority). There is equally a general lack of citizen awareness on data protection and potential data risks though the BOCRA has carried some public awareness through cyber security training and the Cybersmart campaign.

4.1 RECOMMENDATIONS

Based on the aforementioned, the study proposes the following recommendations:

- E-governance should be guided by the adherence to the rule of law.
- There is a need for a rights-based framework that allows ICTs to produce benefits in the public interest and ensure privacy rights are protected pre, during and post PHEIC, as standard data protection regimes and human rights law provide little protection for privacy and responsible data use during times of emergency.
- Fully implement the Data Protection Act by setting up the Information and Data Protection Commission.
- Subject Law enforcement surveillance tools to careful privacy/data protection regulations.
- Intensify public awareness to the public as data subjects on their rights and privacy risks involved in the use of ICTs and newly deployed technologies and appropriate measures to take to ensure the security of personal data.
- Governments in their obligations to respect, protect and promote human rights must be able to ensure that they access only necessary data for public health surveillance and that the measures implemented are legitimate, necessary and proportionate taking into consideration the general data protection principles of transparency, purpose limitation and proportionality- which entails the principal of data minimization.
- Regarding ICT use in future emergency or public health contexts, there should be sensitization on establishing and maintaining a balance between the protection of public health rights and individual rights such as that the individual rights such as privacy are not in jeopardy.

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online): 0493-2137
E-Publication: Online Open Access
Vol:55 Issue:08:2022
DOI 10.17605/OSF.IO/3CA4F

5.1 REFERENCES

Abad, Z. S. H., Kline, A., Sultana, M., Noaeen, M., Nurmambetova, E., Lucini, F., & Lee, J. (2021). Digital public health surveillance: a systematic scoping review. NPJ digital medicine, 4(1), 1-13.

Aiello, A. E., Renson, A., & Zivich, P. N. (2020). Social media–and internet-based disease surveillance for public health. Annual Review of Public Health, 41, 101-118.

Balule, B. T., & Otlhogile, B. (2016). Balancing the Right to Privacy and the Public Interest: Surveillance by the State of Private Communications for Law Enforcement in Botswana. Statute Law Review, 37(1), 19-32.

Bande, L. C. (2018). Legislating against Cyber Crime in Southern African Development Community: Balancing International Standards with Country-Specific Specificities. International Journal of Cyber Criminology.

Blom, P. P., & Uwizeyimana, D. E. (2020) Assessing the Effectiveness of e-Government and e-Governance in South Africa: During National Lockdown 2020. Research in World Economy, 11(5)

Botswana Communications Regulatory Authority (BOCRA) Annual Report 2019.

Botswana Communications Regulatory Authority (BOCRA) Annual Report 2021.

Ferretti, L., Wymant, C., Kendall, M., et al. (2020) Quantifying SARS-Cov-2 transmission suggests epidemic control with digital contact tracing. Science 368(6491).

Frith J and Saker M (2020) it is all about location: Smartphones and tracking the spread of COVID-19. Social Media Society, 6(3), 1–14.

Gasser, U. (2016) Recoding privacy law: Reflections on the future relationship among law, technology, and privacy. Harvard Law Review Forum – Law, Privacy & Technology Commentary Series, 130(2), 61–70.

Google Spain SL and Google Inc v. Agencia Espanola de Proteccion de Datos (AEPD) and Mario Costeja Gonzalez ECLI: EU: C: 2014:317

Gwagwa, A., & Wilton, A. (2014) Protecting the right to privacy in Africa in the digital age. Africa Internet Governance Summit.

Klar, R., & Lanzerath, D. (2020). The ethics of COVID-19 tracking apps–challenges and voluntariness. Research Ethics, 16(3-4), 1-9.

Larsson, H., & Grönlund, Å. (2016). Sustainable eGovernance? Practices, problems and beliefs about the future in Swedish eGov practice. Government Information Quarterly, 33(1), 105-114.

Maalsen, S & Dowling R. (2020). Covid-19 and the accelerating smart home. Big Data & Society, 7(2), 1–5.

Madianou M (2020) A second-order disaster? Digital technologies during the COVID-19 pandemic. Social Media + Society, 6(3), 1–5.

Makulilo, A. B. (2018). The Quest for Information Privacy in Africa. Journal of Information Policy, 8, 317-337

Milne, R & Costa, A. (2020). Disruption and dislocation in post-Covid futures for digital health. Big Data & Society, 7(2), 1–5.

Newlands, G., Lutz, C., Tamò-Larrieux, A., Villaronga, E. F., Harasgama, R., & Scheitlin, G. (2020). Innovation under pressure: Implications for data privacy during the Covid-19 pandemic. Big Data & Society, 7(2).

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online): 0493-2137
E-Publication: Online Open Access
Vol:55 Issue:08:2022
DOI 10.17605/OSF.IO/3CA4F

Nkwe, N. (2012). E-government: challenges and opportunities in Botswana. International journal of humanities and social science, 2(17), 39-48.

Rengel, A. (2014). Privacy as an international human right and the right to obscurity in cyberspace. Groningen Journal of International Law, 2(2).

Riley v. California 573 U.S., (2014)

Sekalala, S., Dagron, S., Forman, L., & Meier, B. M. (2020). Analyzing the Human Rights Impact of Increased Digital Public Health Surveillance during the COVID-19 Crisis. Health and Human Rights, 22(2).

Sohrabi, C., Alsafi, Z., O'Neill, N., Khan, M., Kerwan, A., Al-Jabir, A., & Agha, R. (2020). World Health Organization declares global emergency: A review of the 2019 novel coronavirus (COVID-19). International Journal of Surgery, 76, 71-76.

Wesolowski, A., Buckee, C. O., Bengtsson, L., Wetter, E., Lu, X., & Tatem, A. J. (2014). “Commentary: containing the Ebola outbreak-the potential and challenge of mobile network data”. Public Library of Science Currents, 29(6).

World Health Organization, Global surveillance for COVID-19 caused by human infection with COVID-19 virus: Interim guidance (March 20, 2020).