DATA PROTECTION AND PRIVACY IN NAMIBIA:

AN EXPLORATORY STUDY IN THE CONTEXT OF COVID-19

Internet Society
Namibia Chapter

CIPESA

Data Protection and Privacy in Namibia: An exploratory study in the context of COVID-19

A report compiled by
Nashilongo Gervasius

This report was made possible by funding from the Africa Digital Rights Fund through the Collaboration on ICT Policy for East and Southern Africa (CIPESA).

This report is published by the Internet Society Namibia Chapter pursuant to the Creative Commons Attribution Non Commercial Share-Alike Licence 2.5.

TABLE OF CONTENT

LIST OF ACRONYMS

CRAN:	Communications Regulatory Authority of Namibia
CoE:	Council of Europe
COVID-19:	Coronavirus
DPO:	Data Protection Officer
ESRI:	Environmental Systems Research Institute
E.U:	European Union
GAI:	Generation Africa Intellectual Trust
GDPR:	General Data Protection and Regulation
GPSDD:	Global Partner for Sustainable Development Data
GRID3:	Geo-Referenced Infrastructure and Demographic Data for Development
HILREC:	High Level Research Coordination
IMSI:	International Mobile Subscriber Identity
MICT:	Ministry of Information and Communications Technology
MoHSS:	Ministry of Health and Social Services
MTC:	Mobile Telecommunication Company
NCIS:	Namibia Central Intelligence Service
NFCPT:	Namibia Fish Consumption Promotion Trust
NMH:	Namibia Media Holdings
NSA:	Namibia Statistics Agency
NUST:	Namibia University of Science and Technology
NQA:	Namibia Qualifications Authority
ORDC:	Ongwediva Regional Development Centre
SIM:	Subscriber Identification Module
SMS:	Short Message Service
TN Mobile:	Telecom Namibia Mobile
UNECA:	United Nations Economic Commission for Africa
UNAM:	University of Namibia
WHO:	World Health Organization

Country Overview

Namibia is a democratic country having gained independence in 1990. The southern African country has a population of 2.5 million. It has held democratic elections since the dawn of democracy. Unlike some of her neighbours, Namibia boasts of strong institutions, checks and balances between different arms of the state, respect for human rights and the rule of law. The country also has a very progressive Constitution. The constitution foregrounds the first, second and third generation rights. It is therefore unsurprising that the country is considered a paragon of success when it comes to the promotion and enjoyment of press freedom in Africa.

The right to privacy is provided for under Article 13 of the Namibian Constitution[1] , which states that:

> *"No persons shall be subject to interference with the privacy of their homes, correspondence or communications save as in accordance with law and as is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the protection of health or morals, for the prevention of disorder or crime or for the protection of the rights or freedoms of others".*

Besides the right to privacy being enshrined in the Constitution, its noteworthy to highlight that Namibia does not have a data protection and privacy law at the moment. Attempts have been made by the Namibian government in the last few years to promulgate an Electronic Transactions and Cybercrime Bill in 2017. The Bill received widespread criticism from various stakeholders, which forced the Ministry of Information, Communication and Technology to withdraw the Bill from the public consultation processes. Media reports suggest that the revised Cybersecurity and Cybercrimes Bill will be presented to parliament in the near future. In February 2020, a multi-stakeholder consultation on the Data Protection Bill where 85 participants including government officials, members from telecommunications service providers as well as civil society groups was held in Windhoek, Namibia. Further stakeholder consultations[2] on the proposed Bill took place between September to mid-October 2020 via online platforms by the Ministry of Information, Communication and Technology with the support from the Council of Europe (CoE).

In the absence of a data protection law, incidents of data breaches have become the norm. These data breaches range from corporate[3] to individual level. Because of this state of affairs, Namibia has been referred to as "a safe haven for cybercrime."[4] Consequently, without a cybersecurity and cybercrime law[5] , ordinary Namibians have fallen victim to online fraud[6].

[1] Namibian Constitution, https://www.lac.org.na/laws/annoSTAT/Namibian%20Constitution.pdf, Last Accessed 12 October 2020
[2] 'GLACY+: Stakeholders' Consultation Workshop on the Data Protection Bill in Namibia', https://www.coe.int/en/web/cybercrime/-/glacy-stakeholders-consultation-workshop-on-the-data-protection-bill-innamibia, Last Accessed 12 October 2020
[3] The Namibian, 'SSC leak exposes personal info online', https://www.namibian.com.na/178310/archive-read/SSC-leak-exposes-personal-info-online
[4] New Era Live, 'Namibia a safe haven for cybercriminals', https://neweralive.na/posts/namibia-a-safe-haven-forcybercriminals
[5] The Namibian, 'Cybercrime in Namibia', https://www.namibian.com.na/165301/archive-read/Cybercrime-inNamibia,
[6] NBC, 'Many Namibians fall victim to online fraud',https://www.nbc.na/news/many-namibians-fall-victim-online-fraud.20124

In 2017, the Communications Regulatory Authority of Namibia (CRAN) enforced a provision within the Communications Act of 2009, which requires all mobile phone users to adhere to the provisions of mandatory subscriber identification module (SIM) card registration[7]. Thus, mobile telecommunication operators such as MTC Namibia and TN Mobile were expected to capture demographic data of their users in their databases. The registration exercise was later abandoned after civil society organisations and the media raised concerns[8] . There are media reports that SIM card regulations are under review as part of the on-going review[9] of the Communications Act.

Part 6 of the 2009 Communications Act[10] provides for interception of communications by establishing an interception centre for the purposes of combating crime and national security. For instance, Article 70, (8) reads:

> *"Where any law authorises any person or institution to intercept or monitor electronic communications or to perform similar activities, that person or institution may forward a request together with any warrant that may be required under the law in question to the head of an interception centre."*

There is a general perception among civil society organisations and the media that Namibia engages in intrusive state-sponsored communication surveillance[11]. Reports suggest that this communication surveillance is done by the Namibia Central Intelligence Service[12] as reported by The Namibian newspaper in a detailed three-edition report. [13] [14] [15] Civil society organisations and the media believe that lack of oversight and transparency mechanisms have contributed significantly to the issue of communication surveillance in Namibia. Whilst the technological surveillance capabilities of Namibia remain largely unknown and/or lacking concrete evidence, the fact that the country has acquired a variety of surveillance technologies including International Mobile Subscriber Identity (IMSI) catchers, sophisticated surveillance video cameras and other related smart technologies raises serious concern with regards to how these technologies are being deployed, bearing in mind that part 6 of the Communication Act of 2009 is still not yet in operation[16] .

On the other hand, online violence against women remains a challenge[17]. A report by the World[18] Web Foundation revealed that the lack of cybercrime and data protection legislation in Namibia puts women at risk of online violence, and in vulnerable positions in the cases of non-consensual image sharing (also known as revenge pornography), as well as with regard to online blackmail and sexualised hate speech.

[7]The Namibian, 'Spy agency wants SIM cards registered', https://www.namibian.com.na/163120/archiveread/Spy-agency-wants-SIM-cards-registered
[8]Action Access to Information, 'Ripe for surveillance abuse – Unpacking Namibia's SIM card registration limbo', https://action-namibia.org/ripe-for-surveillance-abuse-unpacking-namibias-sim-card-registration-limbo/
[9]Comms Update, 'Namibia undertakes review of communications law', https://www.commsupdate.com/articles/2019/10/11/namibia-undertakes-review-of-communications-law/
[10]Communications Act, 2009, https://www.nbc.na/sites/default/files/pdf/Namibia%20Communications%20Act%208%20of%202009_0.pdf
[11]https://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/namibia_report_3rd_pages.pdf
[12]Action Access to Internet, 'The rise of the Namibian surveillance state (Part I)', https://action-namibia.org/risenamibian-surveillance-state/
[13]The Namibian, 'The Rise of the Namibian Surveillance State: Part 2', https://www.namibian.com.na/174788/archive-read/The-Rise-of-the-Namibian-Surveillance-State-Part-2
[14]The Namibian, 'The rise of the Namibian surveillance state: Part 3', https://www.namibian.com.na/175475/archive-read/The-rise-of-the-Namibian-surveillance-state
[15]'UPR Stakeholder Submission on the right to privacy in Namibia',
[16]https://privacyinternational.org/sites/default/files/2017-12/Namibia%20UPR_PI_submission_FINAL.pdf https://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/namibia_report_3rd_pages.pdf
[17]Oxford Human Rights Hub, 'Addressing 'Revenge Porn' in Namibia', https://ohrh.law.ox.ac.uk/addressingrevenge-porn-in-namibia/
[18]Internet Society, 'Women's rights online report', http://internetsociety.na/wpcontent/uploads/2020/07/GenderReport-Namibia-FINAL-ONLINE-VERSION.pdf

Definition of Key Terms

Subject/User: This is the individual from whom you wish to gather personal information.

Controller: This is the person responsible for gathering or using information about the subject for a business or organization.

Processor: This is the person who handles the subject's information - storing it, analysing it, organising it, etc. - on behalf of the controller.

Data Protection Officer (DPO): This is the expert you may need to hire to monitor compliance with the GDPR. It's necessary for every public authority, as well as any business or other organisation conducting large scale monitoring of personal data, or monitoring data of a sensitive nature, to appoint a DPO.

Source: Council of Europe

Contextual Background on Data Collection and Covid-19 in Namibia

As highlighted earlier, Namibia does not have a data protection law meaning there are no restrictions on data collection or sharing both at an individual and corporate level. The issue of data collection, processing and sharing have become a topical issue ever since ordinary people and corporates across the world began to digitise all their everyday activities. There is an acknowledgement that personal information is increasingly being collected, processed and shared with third parties without their consent. For instance, revelations by Edward Snowden and the Cambridge Analytica scandal forced the European Union (EU) and other regional blocs to come up with hard and soft laws on data protection.

In Europe, the General Data Protection and Regulation Act (GDPR) has become the model law governing the collection, processing and sharing of personal information with third parties. However, once the global pandemic became real in Namibia, the country was forced to put in place non-pharmaceutical measures such as lockdowns, schooling/working from home, wearing of face masks and social distancing. This unprecedented move was accompanied by the heavy use of digital media technologies for the purposes of work, schooling, shopping and e-commerce payments. Even contact tracing which followed the global pandemic was also reliant on the use of digital technologies. This meant massive data collection, processing and sharing at a time when Namibia had no data protection law in place. Thus, COVID-19 magnified the issue of data collection and transfer in the global South, including in Namibia.

Namibia reported its first COVID-19 cases in March 2020[19] and it was from that point that the government joined hands with various partners to curb further spread of the new coronavirus (COVID-19). The World Health Organisation (WHO) country office became an important stakeholder in providing guidance as the country tried to flatten the curve of the global pandemic. Amongst other interventions, Namibia adopted the contact tracing and surveillance system[20]. Contact tracing is the process of identification of persons who may have come into contact with an infected person ("contacts") and subsequent collection of further information about these contacts.

[19] Namibia confirms two COVID-19 cases https://www.iol.co.za/news/africa/namibia-confirms-two-covid-19-cases-44882925
[20] Namibia: Health Worker in Massive Awe of Contact Tracing Coronavirus Workers https://allafrica.com/stories/202011030209.html

By tracing the contacts of infected individuals, testing them for infection, isolating or treating the infected and tracing their contacts in turn, public health aims to reduce infections in the population.

According to the National Head of Contact Tracing for COVID-19, Ndilimeke Mutikisha, surveillance for Namibia meant getting, "insight into the diverse meaning of how COVID-19 contact tracing data is collected and reported, is vital to understanding the opportunities and challenges to improving public health in COVID times".

In explaining contact tracing, Mutikisha was quoted explaining contact tracing as follows:

> *"By means of an interview, contact tracing healthcare workers engage with COVID-19 positive patients by asking a series of detailed questions to determine level of exposure and risk. First, the latter is asked where they might have picked up the virus. Second, with whom they have been in contact with. Finally, if they may have potentially spread the virus to others. In this sense, information on location and case movement are pivotal when identifying possible hotspots that could erupt and result in fatal cases if prompt action is not taken".*

In the interview extract below, WHO Epidemiologist, Hilary Kagume Njenge provides an early account on Namibia's contact tracing and surveillance practice in Walvis Bay, Erongo region that for month remained an epicentre of COVID- 19[21] transmissions and faced a number of targeted lockdowns. [22] [23] He had this to say:

> *"In collaboration with regional and district administration, and local partners, we were able to identify several hot spots in the Walvis Bay district and start response activities. Some of these hot spots were the Kuisebmund area, the correctional facility and several fishing companies. As a result, over 100 cases were detected and documented within a week. These cases were isolated, and their contacts quarantined. Consequently, this response at Erongo actually proved that Namibia was indeed experiencing community transmission within the Walvis Bay district and urgent attention was required in this district, including the revision of Namibia response strategy and Standard Operating Procedures"*[24]
>
> **(Hilary Kagume Njenge, Epidemiologist at WHO)**

[21] President's Twitter account explaining – COVID-19 Epicenter https://twitter.com/hagegeingob/status/1289266140959707138
[22] Namibia extends COVID-19 lockdown in port town of Walvis Bay to curb community transmissions http://www.xinhuanet.com/english/2020-06/08/c_139124200.htm
[23] Health Alert: Namibia, Walvis Bay Lockdown Measures Expanded To Erongo Region https://www.osac.gov/Country/Namibia/Content/Detail/Report/4cd1e492-4cef-4047-a962-18e3555661b6
[24] WHO (14 August 2020) Heroes from the Namibian COVID health front-line: An epidemiologist's narrative https://www.afro.who.int/news/heroes-namibian-covid-health-front-line-epidemiologists-narrative

However, the COVID-19 reporting and detection protocols in Namibia ignited a lot of conversations on social media were citizens were not happy with the disclosure and collection of personal information as part of contact tracing. Others who were oblivious of the importance of data protection and privacy took to social media urging the government of Namibia through the Ministry of Health and Social Services to set aside privacy and client consent by naming and shaming all those who were infected by COVID-19.

While this call highlighted deep-seated issues of stigma and discrimination associated with COVID-19, it also reveals the cracks in the level of knowledge on privacy matters especially in the digital era where the identity of those named are unlikely to never be forgotten.

In late April, the government of Namibia revised its guidelines on containing the global pandemic. Thus, on 30 April 2020, the President Dr Hage Geingob announced new guidelines[25], which specifically called on businesses to keep clientele log to assist with contact tracing. This was spelt out under section 2 that dealt with Health and Hygiene Guidelines. Immediately after the publication of the guidelines, businesses and public offices around country began taking down people's data for contact tracing and surveillance. The clientele logbook captured information such as names, surnames, phone numbers, place of residence, national registration number and body temperature.

This was done without an enabling legal framework with regards to how the information was going to be kept, shared and data retention period. Thus, these guidelines created a new layer of data collectors and processors in the country at a time discussions were underway about the need to pass the data protection law.

[25]http://www.lac.org.na/laws/2020/GuidelinesforStage2UnderStateOfEmergency_300420.pdf

Data Collection, Contact Tracing and Public Responses

Namibia set up a Contact Tracing Department, which was staffed by mostly health workers. The Head of the COVID-19 surveillance at the Ministry of Health and Social Services (MoHSS), Ms Emmy-Else Ndevaetela, confirmed that her employer decentralised the process of contact tracing . In the end, all the major districts had their own units and heads. Ndilimeke Mutikisha, the National Head of Contact Tracing[26] for COVID-19 in Windhoek said:

> *"I was part of the team that developed the surveillance standard operating procedures, including the design and implementation of surveillance training along with simulation, posters and other learning tools. Additionally, I supported integrated online training for all pillars, where over 600 people were trained across the country. Lastly, I was part of the national team deployed to the Walvis Bay district to investigate community transmission and, set up response structures to control the spread of COVID-19 in the Erongo region. In addition to identifying hot spots within the Walvis Bay district, jointly with my team, we were also able to initiate effective response activities which included working with local stakeholders who in turn mobilized resources for the response"*[27]
>
> **(Ndilimeke Mutikisha, National Head of Contact Tracing for COVID-19)**

In order to conduct effect contact tracing, the Ministry of Health and Social Services and the WHO office in Windhoek enforced rule that people must leave their personal information including names and contact details in a customer register at the front of a public office, retail shop, university and so forth. Furthermore, a government gazette published on 23 September 2020[28] , has set out further measures of contact tracing. However, these measures did not speak to issues of data privacy and protection.

Between March and November 2020, the country witnessed a few digital interventions aimed at collected, soring and processing personal data. With the exception of organisations such as the Namibia Qualifications Authority and Namibia Media Holdings, most businesses, private companies and public offices recorded people's data in physical books. Some organisations and private individuals made effort to create digital contact tracing system, one such example was Joachim Shilongo from Swakopmund[29].

From existing data in place, which include media articles, there was no talk about the implications of collecting, storing, processing and sharing such huge tons of data. Instead of critically engaging with the legal and ethical implications of data collection, media reports on contact tracing focused on the innovative aspects and efficacy of such measures towards curbing the spread of the coronavirus. For instance, the New Era newspaper reported in August 2020 that the High-Level Research Coordination Task force on COVID-19 (HILREC) had developed a contact tracing app[30]. Again, no questions or information on how data was going to be protected on this app was discussed. This partly shows that the media had little interest on the aspect of data protection.

Data Protection: Training, Funding and Regulation during COVID-19

As part of the COVID-19 intervention measures, the government of Namibia received donations from the private sector to 'manage' data and implement effective contact tracing mechanisms. For example, the Namibian office of one of South Africa's largest life

[26] Health experts call on Namibians to trust surveillance and contact tracing system https://www.nbc.na/news/health-experts-call-namibians-trust-surveillance-and-contact-tracing-system.30532
[27] WHO (2 November 2020) Namibia: Health Worker in Massive Awe of Contact Tracing Coronavirus Workers https://allafrica.com/stories/202011030209.html
[28] GOVERNMENT NOTICE No. 233 Public Health Covid-19 General Regulations: Public and Environmental Health Act, 2015 .....https://opm.gov.na/documents/97540/475181/Public+Health+Covid-19+General+Regulations.pdf/fadae86c-0f08-1c38-9ac8-bfc4ffa583ec
[29] Coastal Developer designs tracing sytem https://www.namibian.com.na/202165/archive-read/Coastal-developer-designs-tracing-system
[30] Covid -19 locals develop contact tracing app https://neweralive.na/posts/covid-19-locals-develop-contact-tracing-app

insurance companies - Old Mutual, donated "35 Dell Vostro i7 laptops fully programmed, each with a bag and a mouse, for data capturing, analysis and reporting and 37 Samsung A8.0 tablets for capturing contact tracing data in the field and also for monitoring the contacts, as contact monitoring is mainly done telephonically to avoid unnecessary exposure"[31] . Although training on data protection is considered one of the key pillars of contact training, our research did not found any empirical data on whether health workers, business establishments and restaurant owners received such kind of training prior to the roll out of the new guidelines in April 2020.

In the amended State of Emergency regulations issued on April 17 misinformation was criminalised[32] .

The Amendment Regulations in section 15 read as follows:

> "(1) (e) reads "A person commits an offence if that person - publishes, through any form of media, including social media
> - (i) any false or misleading statement about or in connection with the COVID-19; or
> (ii) any statement that is intended to deceive any other person about the COVID-19 status of any person or measures to combat, prevent and suppress COVID-19 as specified in and under these regulations."

In June 2020, the government amended its state of emergency regulations. The regulations included elements of data protection during COVID-19. Unfortunately, the amendments came three months after the first state of emergency was declared. The regulations provided the following protections[33]:

> (6) The persons who are required to open and maintain a register in accordance with sub regulation (5) must -
> (a) keep the register in a safe place for the duration of the State of Emergency;
> (b) on request, make the register available for inspection by an authorised officer; and
> (c) consider the information provided under this regulation to be confidential, and may not disclose that information to any other person except as provided in paragraph (d) or when required to so disclose in terms of any law.
>
> (7) The register referred to in sub regulation (6) must contain the following particulars in respect of each person who attended the gathering:
> (a) the full names of the person;
> (b) the identification number of the person;
> (c) the nationality and country of residence or origin of the person;
> (d) the physical address of the person;
> (e) the contact telephone or cell phone number of the person; and
> (f) the email address of the person.

For breaking the law, establishments could pay N$ 2000 or face six months imprisonment. It continued to state that:

> 6 (a) requires person(s) to keep the register in a safe place for the duration of the State of Emergency. Sub (c) does state that such 'information' is confidential and may not be disclosed to any other person except as provided in paragraph.

However, such regulations are not binding and questions such as what will happen to such data after the state of emergency needed were not interrogated. The period of data retention was not clearly spelt out.

[31]https://economist.com.na/53938/general-news/old-mutual-donation-to-ease-the-process-of-rapid-case-search-contact-tracing-and-data-management-as-country-battles-covid-19/

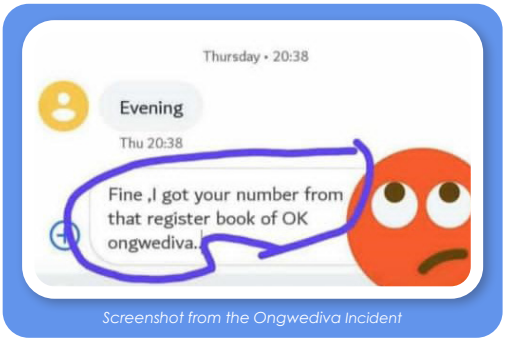
[32]PROCLAMATION No. 13 Amendment of State of Emergency COVID-19 Regulations: Namibian Constitution https://www.lac.org.na/laws/2020/7180.pdf

[33]For a detailed list of the amended regulations during covid-19 in Namibia see http://www.lac.org.na/laws/2020/7250.pdf

Data Exploitation, Targeted Advertising and Women Harassment

Though the amended COVID-19 regulations provided some kind of safeguards against arbitrary collection, sharing, processing and storage of personal data, there was widespread evidence of data breaches, abuse and theft in Namibia during the period under review.

The introduction of public registers at the entrance of private and public buildings was heavily criticised by the media immediately upon its implementation. For instance, the Windhoek Observer lambasted the move arguing that, "Namibia has neither the resources nor the capacity for metadata processing"[34] . In criticising the move, the newspaper further pointed that the exercise was intrusive and exposed people to identity theft. The fear for identity theft was revealed as a reason for why many Namibians were leaving fake names and identities in the registers[35].



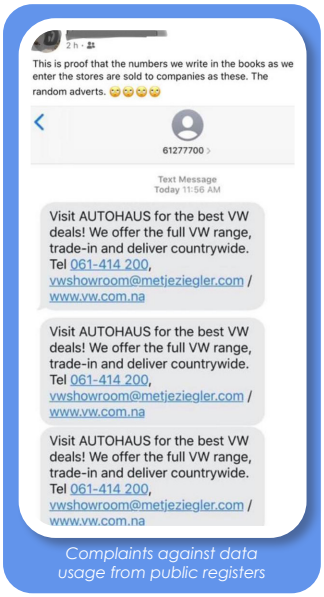
Screenshot from the Ongwediva Incident

The very first case of data breaches surfaced on Twitter in early April when a young woman shared her experience of uninvited contact she received after leaving her personal information at the entrance of a shop in Ongwediva.

While there is no substantive information on whether the young woman took up the case with the police or not, the incident was widely circulated on social media platforms. It highlighted the need for urgent data protection laws in Namibia especially for the purpose of protecting vulnerable young and elderly women.

The incident that took place in Ongwediva confirms the findings of the Internet Society Namibia Chapter that revealed that the lack of cybercrime and data protection legislation in Namibia puts women at risk of violence, and in vulnerable positions in the cases of non-consensual image sharing (also known as revenge pornography), as well as with regard to online blackmail and sexualised hate speech.

Another COVID-19-related incident is one narrated by *Mary Haufiku who posted on her Facebook page in early April, 2020 highlighting her concern about the usage of her data when she left it at a public building. She revealed how a certain car dealer bombarded her with targeted advertisements after leaving her information at the entrance of a shop, as illustrated in Figure 3.



Complaints against data usage from public registers

As if that was enough, The Namibian newspaper in November 2020 published a story whereby "a COVID-19 customer register was allegedly stolen from the Namibia Fish Consumption Promotion Trust (NFCPT) shop at Ondangwa by unknown suspects" . This case of stolen data highlighted the precarious nature of personal data in the absence of an enabling legislative framework. Ever since the publication of the news article, there hasn't been any follow-ups or enquiries on this case making it a challenge to fully track its progress.

Another unrelated data issue that occurred during COVID-19, was reported by the Namibian Sun in October 2020 reported that 25 government websites were hacked and defaced by anonymous people . In response, a media statement from the Office of the Prime Minister denied this saying that several government websites were down between 8 and 9 October 2020 largely due to unforeseen technical problems .

[34] https://www.observer24.com.na/as-expected-sign-in-books-are-a-waste-of-time/
[35]https://www.namibian.com.na/96668/read/First-name-Apple-last-name-Tomato
[36] Internet Society, 'Women's rights online report', http://internetsociety.na/wpcontent/uploads/2020/07/GenderReport-Namibia-FINAL-ONLINE-VERSION.pdf

Events such as these, however, foreground the vulnerability of personal and classified data stored in government servers and websites, which could easily be stolen by hackers in the absence of data protection law.

COVID-19, Digital hub and Data Protection

In September 2020, the Ministry of Health and Social Services, the United Nations Economic Commission for Africa (UNECA), the Environmental Systems Research Institute, the Global Partner for Sustainable Development Data, GRID3 and the Namibia Statistics Agency (NSA) launched an online COVID-19 Information Hub. Although it is available to the public, the hub does not contain personal data. However, it only contains statistics, graphs and infographics on COVID-19 cases in Namibia. There is no information about data protection or how citizens and retail shops can protect their data on the hub. There is no information on what happened to the logbooks from retail shops and various establishments containing people's personal data and information collected at the height of the global pandemic.

However, videos with customer's data have circulated on TikTok and WhatsApp. This shows how easy it is for citizens and businesses to access and misuse personal data. Data owners have also been complaining on social media about how business entities that previously did not send them adverts through SMS have suddenly began doing so during COVID-19. There is a widespread that businesses are using the clientele logbooks processed during COVID-19 for advertising purposes. Thus, instead of using information strictly for contact tracing, the data has been monetised and repurposed for ulterior business purposes. There is no protection of personal data at different business establishments. This has made easy for people to scan through contact details of customers at various private and public offices.

Methodological Approach

Given the contextual background articulated above, this study sought to understand how the data was collected, processed, stored and shared at the height of the global pandemic in Namibia. In order to make sense of this issue, the study relied of various qualitative data collection instruments such as semi-structured interviews, document analysis and face-to-face interviews with key informants, data collectors and ordinary people in Namibia. Data was collected between March and November 2020.
Additionally, we conducted an online survey was conducted for three weeks between October and November 2020 with data owners, collectors and processors, members of the civil society and academics (see appendix for semi-structured questions for data owners, data collectors and civil society).

The survey was conducted with the aim to assess the level of awareness of data protection and privacy in Namibia amongst different players in the data protection and privacy ecosystem and in total, 140 responses have been recorded for this survey. The survey also provided an opportunity for data owners to convey their most pressing worries about data protection and privacy during the period of COVID-19 enforced regulations. The survey was split into four categories, for data owners, data collectors/processors, data regulators as well as the civil society and the academic community.

DATA INTERPRETATION AND ANALYSIS

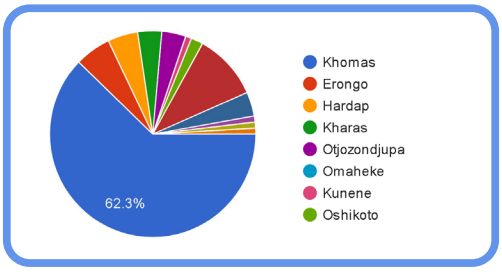
Researching Data Privacy and Protection in Namibia during COVID -19

As discussed above, for a period of three weeks between October 18 and November 6th, we ran an online survey with the aim to assess the level of awareness of Data Protection and privacy in Namibia amongst different

[37] https://www.namibian.com.na/96223/read/Covid-19-customer-register-stolen
[38] https://www.namibiansun.com/news/hackers-take-aim-at-namibia2020-10-09
[39] https://www.namibianewsdigest.com/opm-rejects-claims-that-government-servers-were-hacked/

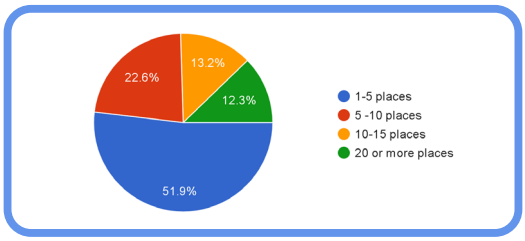
players in the data protection and privacy ecosystem. The survey also provided an opportunity for data owners to convey their most pressing worries about data protection and privacy during the period of COVID-19 enforced regulations. The survey was split into four categories, for Data owners, data collectors/processors, data regulators as well as the civil society and the academic community.

Our online survey for members of the public (or data owners in this case), received 106 responses whom 71.7 percent were female and 28.3 percent were males. Namibia being a country with 14 political regions, our survey recorded 62.3% responses from Khomas region where the capital city of Windhoek is located.



Geographical representation of respondents

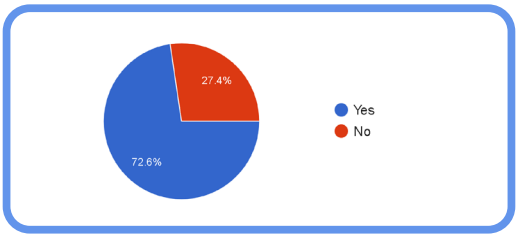
As the COVID-19 pandemic sought to restrict movement and encouraged people to stay home, our first survey question asked survey participants to retrace their movements with data protection in mind and reflect as to how many places they have visited and consequently left their data. The data owners also responded that they had left personal data either at the shops or other service provision places with over 50% of respondents confirming that they shared their personal data at either one or five shops. At least 22.6 percent indicated that they left it in about or less than 10 places, 13.2% at 15 different places and 12.3 percent at 20 different shops or places and more.



Indication of # of places respondents have visited a week before

In exploring the level of awareness for data usage, 79.2% revealed that they were extremely concerned about how their personal data is being used by data processors when they leave it in the public domain. They feared being victims of online crimes as well as stalking.

Our research also showed that 72.6 % of the respondents had entered accurate information as requested by the state guidelines through the public registers and only 27.4 % were hesitant to provide full and accurate information in this exercise. These results highlighted the level of awareness on the importance of data protection and privacy in the country.

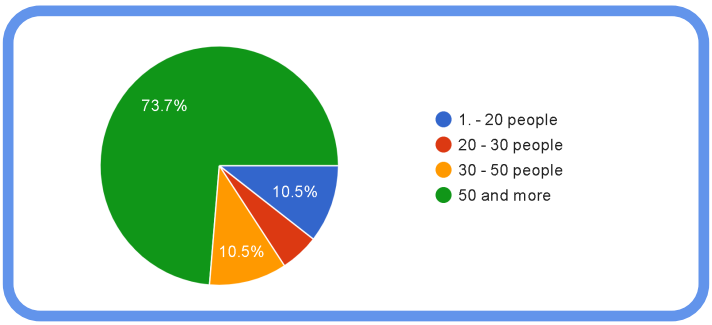


Responses to the usage of genuine information in COVID-19 public registers

However, respondents who reported to have had provided wrong and inaccurate data in public registers justified their actions by quoting "privacy issues", "not knowing where their information where going to", "not being comfortable sharing their names and identification numbers with anyone", "being afraid to be admitted into isolation facilities based on the rumours around the unstable facilities conditions" as amongst the reasons behind their actions.

Other reasons raised by respondents include: "fear of scammers having access to their details", fraudulent activities being carried in their names, and "identity theft and harassments" .

On their side, the data processors/collectors who in this case included shop owners/managers and security guards, confirmed during this time that on a daily basis more than 50 people were leaving their private data at the shops but also revealed that 87% of their customers exhibited unwillingness to leaving their data at the shops.



Data Processors responses to the number of clients having entered their premises in the past week

On the question of whether the data collectors had received training on the privacy and protection of the information in the public register books, 90% of the respondents indicated they have not been trained by any institution on how to handle personal data and information, nor did they knew of immediate or plans within 5 months regarding the usage of registers and information they contain. With regards to who has access to the public registers, the majority of our respondents indicated that their managers, supervisors, administration staff as well as the floor managers had access to the public registers. They also kept the registers when they are full.

For the sub-category targeting the academia and civil society under the theme of research and human rights; the respondents indicated that the biggest concerns associated with public data collection accompanied COVID-19 interventions were issues of privacy, indiscriminate harvesting of data and the fact that the data could be viewed by anyone.

The lack of proper public education on data protection and privacy was listed as one of the major issue concerning the use of public registers. Others indicated the issue of the increased case where phone numbers of members of the public were being used for committing crimes. One respondent observed that there was the "abuse of COVID19 as a cover-up to collect data from the public, for political or economic purposes" as reason for concern in the data collection and handling process.

Data that was collected on print papers is not of much concern, but the one that was collected through mobile app and other comprised systems can easily be repurpose, unless if it was made mandatory to discard such data after every two weeks as contact tracing was only effective for a two weeks period

People have to sign in with their personal details when entering shops and other official places. Those information including personal identification numbers could fall into the hands of fraudsters and be used to apply for things like passports and credit cards.

It was not clear how some of the data collected by shops was related to contact tracing, for example, I don't see the need of asking for one's nationality for you to be able to enter a shop.

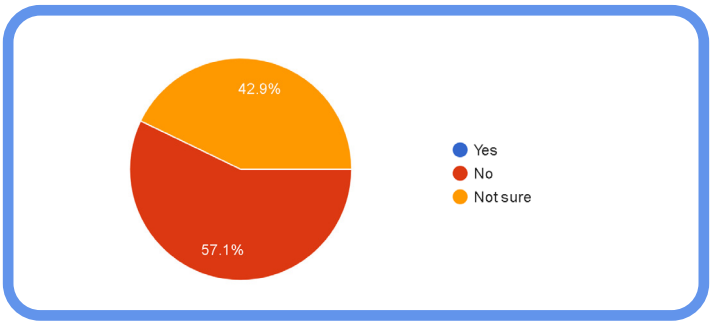
Inaccessibility to information at public, Civil Society, and private sector level.

The security of the collected data as there are no data protection laws and measures on place. The collected sate can be used by anyone anyhow including being sold on the dark market.

All is about lack of TRUST of ordinary people to what the ones in power (locally & globally) are capable of.

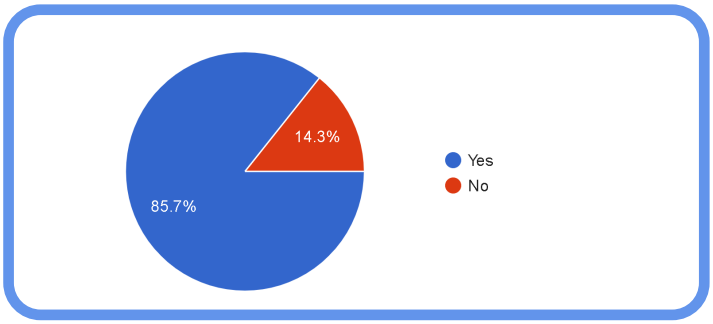
1) there are data manipulations to influence populations to blindly accept public instructions...
2) there is increase subordination of nations to global order related powers e.g. New Order.

Surprisingly enough, even amongst this group of respondents which is perceived to be highly knowledgeable on a wide range of issues; many of them were not aware of the existence of data protection law in the country. They responded to the following question: "Is there any data protection law or regulations governing this unprecedented collection of public data by shops, malls and offices?



CSO & Academia knowledge of the existence of Data Protection Law in Namibia

Over 80% of this group justified the use of fake or pseudonyms by members of the public when entering shops or public offices. They explained that such behaviour is warranted given that the information is not being collected in the public interest.



Responses to whether usage of fake names and pseudonyms are justifiable in public registers CSO & Academia knowledge of the existence of Data Protection Law in Namibia

Respondents believed that using fake and pseudonyms is warranted, as "skepticism about potential data abuse would push people to use pseudo data". One respondent added that, "the worse was that people could even impersonate others by using data of other people". The respondent added saying that, "this unfortunately was brought by the fact that there wasn't measure to mitigate possible data misuse".

Respondents also supported members of the public arguing that pseudo identities help them to protect their identities in a world full of uncertainties. One respondent highlighted that because there is no law protecting personal data, leaving it in the plain view to other customers leave the onus with the individual data owners to decide if they want to share their real details or not and how they share it as most information does not get used intended purpose. In support of the cited reasons, others believed the reasons below are valid enough for the public to use fake names in the public registers.

They had this to say:

People don't have to give their personal details because it might fall into the wrong hands and be used for harming individuals in many ways. And the shops might target individuals with spam advertisements.

People use that info to call. I used to get crazy calls from people I didn't know until I suspected it's those forms. I stopped giving full # and calls stopped".

One cannot publicly share sensitive information when they know it can be misused. However this affects the efforts to trace contacts negatively.

Main stream media and official news rooms tell what they are instructed to say... they do not care that we are in a global village where nothing will remain hidden! Are they not the actual conspiracy theorists?

However, 14% of the respondents that believed that the act should not be warranted. Some of them, explained it as follows:

What is vital is the contact number for tracing purposes not the real name.

No, there is a premise for public offices to collect information from the public, as long as it benefit the public in the long term.

When asked to recommend the most safe and secure ways for data collectors and processors in Namibia, respondents felt that, "collected data during this time needed to be shredded or burned after the lapse of two weeks from the day filled as they can help in making sure that the data are not all over the place and ending up being in the possessions of wrong people." Another respondent also observed that, "there is a need for digitizing data across all sectors as well as educating data collectors on keeping data safe and secured". In the words of another respondent "More transparency is needed in communicating why the data is being collected, equally important, members of the public need to be given and option in regards to participation. In other words they should be given the choice to participate or to withhold their information".

Further recommendations proposed by the respondents are as follows:

They must inform people how they will protect and store such sensitive information.

Use encryption and password secure devices

Make sure that data is digitally stored and collected.

Ensure that data is auto deleted after 3 weeks from collection.

Digitising data across all sectors will be a good start.

More training is needed for data collectors

Citizens must carry their national documents at all time for confirmation purposes

Use protected digital devises that only a few people have access to the data

The papers being completed need to be stored safely

Books must be closed or rather use scanners so that no one will see others' information

Use only names without surnames and ID numbers

Use scanners on IDs, or other electronic means that protect the data from plain view

Actually nothing! Given the state of affairs of present humanity

Perhaps use more scanning devices instead of book signing that everyone has access to

Approximately 77 percent of this group of respondents felt that the proposed Data Protection Bill currently in formulation must be quickly finalised to safeguard ordinary citizens from arbitrary abuse. They felt that the finalisation of this document would assist in safeguarding citizens data, while 23.1% responded a "no" to this question that didn't provide an option for reasons behind the no.

Recommendations

This study explored varied degrees of data protection and privacy in Namibia in the context of COVID-19. Additionally, the study also carried specific surveys targeting different players in the data ecosystem. Hence the study proposes the following recommendations for the different players.

Government

- Though the Ministry of Information and Communication Technology is in the process of drafting the Data Protection law, there is a need to speed up the finalisation of the bill and use lessons learned from the COVID-19 pandemic to come up with a progressive piece of legislation.
- Upon passing the law, ensure comprehensiveness that hold companies accountable for how they collect and use people's personal information.
- There is need to limit the role of data handlers and keep the national statistics agency as well as the Ministry of Health and Social Services to be more involved in the training and preservation of the data related to COVID-19 which was collected at various business establishments, private and public offices.
- For National exercise requiring data collection, government should work on public trust in ensuring the safety of data.
- Ensure ease of access for public to report concerns about their data on the service and address concerns in a timely manner
- Civil Society Organisations
- Public education and awareness needs to be prioritised on how personal data is collected and disseminated, and can be protected.
- CSO must get involved in all processes of the bill to arrest any potential infringement to society

Data Processors

- Training on data handling must be prioritises at all levels of data processing by various processors.
- Explore with other business models that strengthen data rights , respect privacy and minimise data collection practices

Data Owners

- Must continue questioning the usage of their data by data handlers and processers and take action by lodging public complaints when breach has happened
- Demand for control on managing their own data when using online platforms.
- Media
- There is a need for the media in Namibia to be sensitised on this topic in order to better inform the public on their rights on data usage and protection when it involves third parties.
- Media should be equipped with knowledge of different aspects of data handling in a digital world
- There is also a need for media to be equipped with knowledge on technology and innovation to be able to effectively inform the public of how these relate to them, their rights, and their being

Academia

- Natural and social scientists need to work together to set guidelines that better protect personal data in Namibia.
- HILREC must propose guidelines on data protection in the context of contact tracing that have become the norm during COVID-19.

Conclusion

In conclusion, our research found that most data collectors were harvesting public data through public registers without proper any training on data protection and privacy. Additionally, our research has found no evidence of the Namibian Statistics Agency (NSA) actively working on data management and training of data usage during COVID-19 with public facilities ensured with data collection during this period and as a result, healthcare workers and the public had to manage the data themselves.

Our research has also found that the public had no confidence in this process that resulted in many providing fake details and pseudonyms when filling in public registers at private and public spaces. This study confirms the need for the country to finalise the Data Protection Bill so that the public can be protected from arbitrary abuse by data collectors and processors.

The usage of public data beyond the COVID-19 period also raised serious concerns amongst members of the public. They complained that they had never been contacted from the shops and other public establishments despite leaving their personal information. They felt the exercise was meaningless. The security of the public data recorded using technological applications is also unknown leaving this tons of data even more susceptible to abuse in a long run especially given the fact that there is no enabling legal framework. The general lack of awareness on data protection and privacy amongst members of the public side can be attributed to lack of involvement in public awareness by civil society organisations. There is little discussion around this issue by the state broadcaster like the Namibia Broadcasting Corporation.

It is also concluded that COVID-19 brought with it a coterie of data collectors and processors. These processors were however operating outside an enabling legislative framework. It revealed that media did not engage or interrogate issues relating to personal data protection in their reportage. They also failed dismally to highlight the inherent dangers that exist in the invasive collection and processing of personal information.

APPENDICES

Questionnaires used for online survey hosted via Google Drive from October 18 to November 6th

Appendix 1

Data Protection and Privacy Questionnaire for Individuals/Data Owners October 18 – Nov 6th.

Africa Digital Rights Fund – Namibia Project

Individuals/Data Owners:

1. How many places have you left your data at in the last 5 days?

*1-5 places *5 -10 places * 10-15 places *20 or more places

2. To what extent are you concerned/ worried about how this information is being used by data processors when you leave it there?

*Not worried *somewhat worried *very worried

3. Do you always share the correct information at the entrance of the shop or malls when asked about your name, mobile phone number and ID details?

4. Have you ever shared incorrect information to the data collectors? If so, what is your justification?

5. What is the biggest fear you have about leaving your data in public places?

6. If you are given an opportunity to ask any questions to those handling your data beyond the shop, what would you ask them?

Appendix 2

Data Protection and Privacy Questionnaire for Data Processors/Collectors (Shop Owners/ Managers/Security Guards - October 18 – Nov 6th.

Data Processors/Collectors (Shops Owners/Managers/Security Guards)

1. On a daily basis, how many people leave their contacts here?

2. How would you rate the level of willingness to leave information in the books by clients or those seeking services here?

*Moderately willing *very willing *not willing at all

3. Have someone tried to take pictures of the registers or the entire book once or more before?

4. Where do you keep the books when they are full?

5. Who has access to them?

6. What are the plans with these registers and the information they contain in the next 5 months?

Appendix 3

Data Protection and Privacy Questionnaire for Civil Society & Members of the Academia - October 18 – Nov 6th.

QUESTIONAIRE FOR CIVIL SOCIETY/ACADEMIA

1. What are the biggest concerns associated with public data collection that has accompanied COVID 19 interventions?

2. Is there any data protection law or regulations governing this unprecedented collection of public data by shops, malls and offices?

3. Members of the public are said to be using their fake or pseudonyms when entering shops or public offices. Do you think such behavior is warranted given that the information is being collected in the public interest?

4. What can be done by data collectors and processors in Namibia to ensure that the data that is being harvested is secure, safe and confidential?

5. Namibia is busy working on the Data Protection Bill. Do you think this law will be able to provide the necessary safeguards against abuse?

Appendix 4

Data Protection and Privacy Questionnaire for Government institutions - October 18 – Nov 6th.

- Ministry of ICT
- Ministry of Health and Social Services
- Ministry of Justice
- Communications Regulatory Authority of Namibia

QUESTIONNAIRE FOR GOVT/MICT/MOHSS/MOJ/REGULATOR

1. There have been incidences of data breaches and violations during COVID 19. What are some of the driving factors of these breaches?

2. There have been people who have harassed or trolled as a result of leaving their data at public places. What can be done to ensure these people can seek recourse/ justice?

3. Can you explain to us what does the law say about data retention period for data collectors and processors during this time of COVID-19?

4. How can the public seek recourse when their data has been abused by third parties?

REFERENCES

Action Coalition (2018). The rise of the Namibian surveillance state (Part I), retrieved from https://action-namibia.org/risenamibian-surveillance-state/

African News Agency. (2020). Namibia confirms two COVID19 cases. retrieved from https://www.iol.co.za/news/africa/namibia-confirms-two-covid-19-cases-44882925

All Africa. (2020). Namibia: Health worker in Massive Awe of Contact Tracing Coronavirus Workers, retrieved from https://allafrica.com/stories/202011030209.html

Amukeshe. L, (2020), Coastal Developer Designs Tracing System, The Namibian, retrieved from https://www.namibian.com.na/202165/archive-read/Coastal-developer-designs-tracing-system

Carter. M, (2020). Old Mutual Donation to ease the process of rapid case search, contact tracing and data management as country battles COVID-19, *Namibia Economist*, retrieved from https://economist.com.na/53938/general-news/old-mutual-donation-to-ease-the-process-of-rapid-case-search-contact-tracing-and-data-management-as-country-battles-covid-19/

COMMS Update. (2019). Namibia Undertakes review of communications law, Retrieved from https://www.commsupdate.com/articles/2019/10/11/namibia-undertakes-review-of-communications-law/

Council of Europe. (2020). Stakeholders Consultation Workshop on the data protection Bill in Namibia, retrieved from https://www.coe.int/en/web/cybercrime/-/glacy-stakeholders-consultation-workshop-on-the-data-protection-bill-in-namibia

Geingob. H. (2020). Covid19 Epicenter, Retrieved from https://twitter.com/hagegeingob/status/1289266140959707138

Immanuel. S and Ngutjinazo. O, (2018), SSC leak exposes personal info online, *The Namibian*, retrieved from https://www.namibian.com.na/178310/archive-read/SSC-leak-exposes-personal-info-online

Legal Assistance Centre (2014). Namibian Constitution, retrieved from https://www.lac.org.na/laws/annoSTAT/Namibian%20Constitution.pdf

Legal Assistance Centre. (2020). Detailed list of the Amended Regulations during COVID-19 in Namibia, Retrieved from http://www.lac.org.na/laws/2020/7250.pdf

Legal Assistance Centre. (2020). Proclamation No. 13, Amendments of State of Emergency COVID-19 Regulations: Namibian Constitution, retrieved from https://www.lac.org.na/laws/2020/7180.pdf

Legal Assistance Centre, (2020). Guidelines for stage 2 under State of Emergency, Retrieved from http://www.lac.org.na/laws/2020/GuidelinesforStage2UnderStateOfEmergency_300420.pdf

Links, F. (2020), Ripe for Surveillance abuse-Unpacking Namibia's SIM card registration limbo, Retrieved from https://action-namibia.org/ripe-for-surveillance-abuse-unpacking-namibias-sim-card-registration-limbo/

Links, F. (2018), The rise of the Namibian surveillance state: Part 3, The Namibian Retrieved from https://www.namibian.com.na/175475/archive-read/The-rise-of-the-Namibian-surveillance-state

Links, F. (2018), The rise of the Namibian Surveillance State: Part 2, The Namibian, Retrieved from https://www.namibian.com.na/174788/archive-read/The-Rise-of-the-Namibian-Surveillance-State-Part-2

Mare, A. (2019). Communication Surveillance in Namibia: An Exploratory Study, Media Policy and Democracy Project, retrieved from https://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/namibia_report_3rd_pages.pdf

Ministry of Information, Communication and Technology, (2009). Communications Act, 2009, retrieved from https://www.nbc.na/sites/default/files/pdf/Namibia%20Communications%20Act%208%20of%202009_0.pdf

Namibia Press Agency, (2020). OPM Reject Claims that Government Servers where Hacked, retrieved from https://www.namibianewsdigest.com/opm-rejects-claims-that-government-servers-were-hacked/

Namibian Sun (2020), Hacker Take Aim at Namibia, Retrieved from https://www.namibiansun.com/news/hackers-take-aim-at-namibia2020-10-09

Nakale, A. (2020). Covid-19: Locals develop contact tracing app, *New Era*, Retrieved from https://neweralive.na/posts/covid-19-locals-develop-contact-tracing-app

Nashuuta. L, (2018) Namibia a Safe Haven for cybercriminals, New Era, Retrieved from https://neweralive.na/posts/namibia-a-safe-haven-for-cybercriminals

NBC, (2020). Health Experts call on Namibians to trust surveillance and contact tracing system, Retrieved from https://www.nbc.na/news/health-experts-call-namibians-trust-surveillance-and-contact-tracing-system.30532

Nembwaya. H, (2020), Covid-19 customer register stolen, The Namibian, Retrieved from https://www.namibian.com.na/206001/archive-read/Covid-19-customer-register-stolen

Ndeunyema. N, (2015), Addressing Revenge Porn In Namibia, Oxford Human Rights, Retrieved from https://ohrh.law.ox.ac.uk/addressing-revenge-porn-in-namibia/

Olivier, F, (2017). Cybercrime in Namibia, The Namibian, Retrieved from https://www.namibian.com.na/165301/archive-read/Cybercrime-inNamibia

Office of the Prime Minister, (2020), Government Notice No: 233 Public Health Covid-19 General Regulations: Public and Environment Health Act, 2015, retrieved from https://opm.gov.na/documents/97540/475181/Public+Health+Covid-19+General+Regulations.pdf/fadae86c-0f08-1c38-9ac8-bfc4ffa583ec

Privacy International, (2015). The Right to Privacy in Namibia, Retrieved from https://privacyinternational.org/sites/default/files/2017-12/Namibia%20UPR_PI_submission_FINAL.pdf

Seibeb.E, (2018). Many Namibian fall victim to online fraud, Namibia Broadcasting Corporation, Retrieved from https://www.nbc.na/news/many-namibians-fall-victim-online-fraud.20124

The Namibian (2017) Spy Agency wants SIM cards registered, retrieved from https://www.namibian.com.na/163120/archive-read/Spy-agency-wants-SIM-cards-registered

U.S Embassy Windhoek (2020), Health Alert, Namibia, Walvis Bay. Lockdown Measures Expanded to Erongo Region, retrieved from https://www.osac.gov/Country/Namibia/Content/Detail/Report/4cd1e492-4cef-4047-a962-18e3555661b6

Internet Society Namibia, (2020). Namibia Women's Rights Online, retrieved from https://isocnamibia.org/wp-content/uploads/2020/07/AGENDA-Namibia-Women-Rights-Online-Report-Launch-FINAL.pdf

WHO (2020), Heroes from the Namibian COVID health front-line: An Epidemiologist's narrative, retrieved from https://www.afro.who.int/news/heroes-namibian-covid-health-front-line-epidemiologists-narrative

Windhoek Observer, (2020). As expected sign –in books are a waste of time, retrieved from https://www.observer24.com.na/as-expected-sign-in-books-are-a-waste-of-time/

UNICEF, (2020) Digital tracing and surveillance during COVID-19, retrieved from https://www.unicef-irc.org/publications/pdf/WP2020-01.pdf

Xinhua. (2020). Namibia extends COVID-19 lockdown in port town of Walvis Bay to curb community transmission, Xinhua. retrieved from http://www.xinhuanet.com/english/2020-06/08/c_139124200.htm

Internet Society
Namibia Chapter

CIPESA