Department of International Development

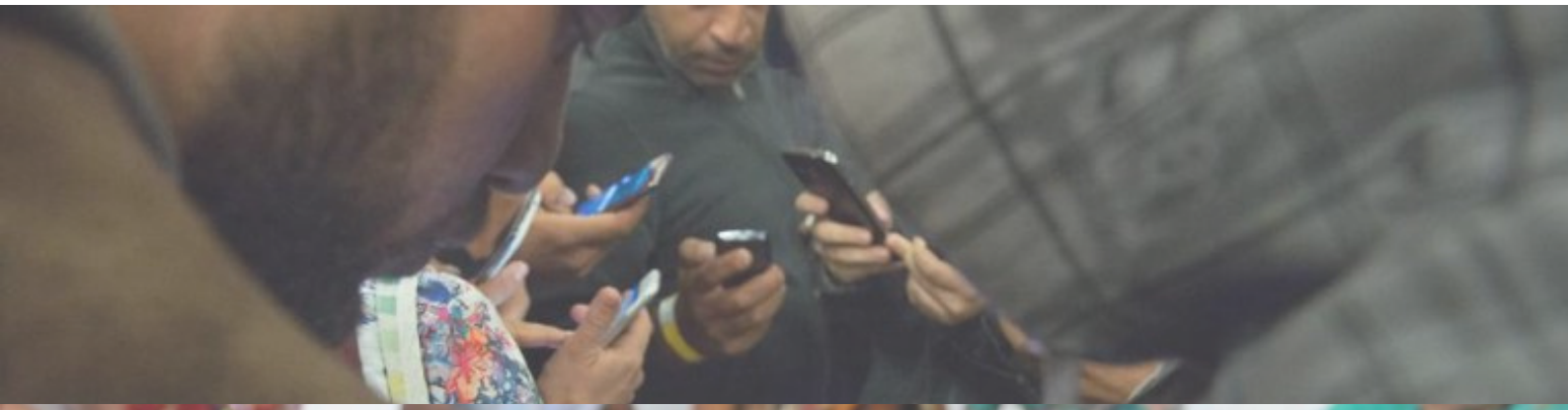
VALENTINE BOTTERI
MADELINE COPP
ANA CAROLINA MUÑOZ-MORALES
IRINA REKHVIASHVILI

GOVERNMENT RESPONSES TO THE COVID-19 PANDEMIC

IN AFRICA, LATIN AMERICA, SOUTHEAST ASIA AND MIDDLE EAST

IN PARTNERSHIP WITH AWO AGENCY

MARCH 2021



Acknowledgements

We would like to express our special thanks to the Development Management teaching team at the London School of Economics and Political Science, especially to our mentor for this project, Dr. Moritz Schmoll. We would also like to thanks AWO Agency for allowing us to collaborate with this consultancy work, we are particularly thankful to Sophie Clavet and Aparna Surendra for their guidance and frequent feedback. Lastly, we would like to acknowledge the members of civil society organizations that contributed to this work with their valuable time, knowledge and perspectives.

Government responses to the Covid-19 pandemic in Africa, Latin America, South East Asia, and the Middle East

Abstract

Contact tracing apps were part of the response to the pandemic worldwide; however, these initiatives raised concerns related to human rights, and particularly to privacy issues. This report examines the Covid-19 apps that were developed and adopted as public health measures in Africa, Latin America, Southeast Asia, and the Middle East. It undertakes a technical assessment in nine countries where the apps have been rolled out, examining this process in light of their national privacy ecosystem. This report concludes that technological solutions to fight the pandemic have double-edge effects, as certain public health measures can turn into opportunities for human rights violations and the lack of comprehensive data protection laws and enforcing authorities remains a challenge. It provides policy recommendations in four key areas: accountability, transparency, proportionality and human rights.

Table of Contents

Introduction

The Covid-19 pandemic led governments from all over the world to look for innovative ways to contain the spread of the virus. Contact tracing mobile applications (hereafter apps) were among the most relevant digital initiatives introduced. Nevertheless, this strategy prompts a series of caveats particularly in low- and middle-income countries where regulations on privacy and data protection are relatively new, less specialized or not effectively enforced, and where civil liberties are on occasions weakly protected. The use of apps – often collecting location and sensitive information – without clearly defined regulatory frameworks raises potential privacy issues. In addition, the pandemic led to the activation of emergency protocols that expand the capacities of the state – even at the expense of fundamental rights – for outbreak containment purposes without explicit boundaries or proportionality evaluations.

Expanded state powers, as well as the potential use of security infrastructure to contain the spread or the use of public health initiatives for security objectives, pose the risk of apps becoming securitizing tools. Therefore, the interaction of factors such as privacy regulations and enforcement, apps' technical features, emergency protocols, and the susceptibility of specific populations to social control create different degrees of vulnerability, accountability and control in low-capacity settings. This report examines Covid-19 apps deployed in Africa, Latin America, Southeast Asia, and the Middle East, and their potential implications for privacy. It identifies key technical features, investigates evidence of "function creep" or data misappropriation, examines the apps' impact on human rights of citizens, particularly on vulnerable populations, and provides policy recommendations.

Digital contact tracing as a public health measure

Non-pharmaceutical interventions, particularly containment and mitigation strategies, were among the main public health responses to the Covid-19 pandemic, given the absence of immunization and effective treatment during early stages. Containment and mitigation measures

aimed to suppress and slow down the outbreak in order to avoid the overload of health systems (OECD, 2020). These interventions are crucial for timely outbreak control in low- and middle-income countries due to their weaker healthcare capacities (Kandel et al., 2020). Contact tracing is among the most relevant containment strategies as it makes it possible to identify infected persons before any symptoms appear. However, contact tracing is labor-intensive, since it requires high coordination with testing systems and robust capacity to contact at least 36 people for every positive case (Keeling, Hollingsworth & Read, 2020). Moreover, the extent of contact tracing is determinant in the efficacy of this measure and it has been suggested that to achieve outbreak control, up to 80% of population should be traced (Kretzschmar et al., 2020).

Digital solutions emerged as a response to these difficulties. Mobile applications were created to support and, in some cases, replace, analogous contact tracing. However, evidence of effectiveness remains heterogeneous; there are claims that the acceleration of the tracing process facilitated by the app would increase effectiveness and drop the coverage requirements by up to 20% (Kretzschmar et al., 2020). On the other hand, others argue that the limited reach of apps makes digital tracing ineffective (Kucharski et al., 2020). These considerations are particularly relevant in the context of low and middle income countries, since access to the internet and digital technologies is either low or highly unequal (ITU, 2018), raising further questions about the real effectiveness of contact tracing apps.

Privacy and Covid-19 Apps

Multilateral organizations, civil society, data protection authorities and academics have highlighted individual privacy concerns and considerations (Bengio et al., 2020; UN General Assembly, 2020; Gasser et al., 2020). These organizations ask whether surveillance solutions like contact tracing apps are necessary, proportionate, and lawful (UN General Assembly, 2020; Amnesty International UK, 2020; Gasser et al., 2020).

While contact tracing is privacy invasive, it is typically considered necessary as a public health solution (UN General Assembly, 2020). However, while manual contact tracing is deemed proportionate, organizations have questioned the proportionality of apps that grant continuous

access to devices or monitor location through geolocation (UN General Assembly, 2020). While all apps threaten data privacy by requiring access to health status, behavior, or location, digital tools that measure spatial proximity or use aggregate mobile phone tower data are viewed as less invasive than personal contact tracing, quarantine enforcement apps, or GPS data apps (Gasser et al., 2020).

Governments have enabled measures and data collection to limit the spread of Covid-19 that would not typically be justified (UN General Assembly, 2020; Gasser et al., 2020; Zwitter & Gstrein, 2020; CoE, 2020). To ensure privacy, the UN Special Rapporteur recommends that governments incorporate the standards of Convention 108[1] into their legal systems before enabling any solutions (UN General Assembly, 2020). These legal frameworks should provide oversight on the purpose, collection, analysis, storage, and erasure of data (Zwitter & Gstrein, 2020).

Civil society and multilateral organizations have highlighted a number of privacy concerns including: how the app gathers location data (UN General Assembly 2020); whether the data is stored in a centralized or decentralized manner (ibid.); whether there are clear privacy policies in place (Bengio et al., 2020); whether the data is time-bound and deleted after the pandemic (ibid.); whether it is voluntary (Morley et al, 2020); and whether it is purpose-limited to Covid-19 (ibid.).

Securitization and Emergency Measures

Securitizing public health measures has become relatively common in recent years. The Copenhagen School of academic thought defines securitization as a "successful speech act through which an intersubjective understanding is constructed within a political community to treat something as an existential threat to a valued referent object and to enable a call for urgent and exceptional measures to deal with the threat" (Buzan and Wæver, 2003). The theory essentially states that an issue becomes a threat when an actor declares it as a national security concern and portrays it as an issue of supreme priority, thus justifying the use of emergency measures. This

[1] Convention 108 is an international Council of Europe treaty that protects individuals against privacy abuses related to the collection and processing of personal data and outlaws the collection of sensitive data.

analytical approach has been used to analyze many recent epidemics, from SARS to MERS and Zika virus among others, but nothing on the scale of the Covid-19 pandemic (Nunes, 2020).

Every country around the globe introduced a variety of containment measures from quarantines to lockdowns and nighttime curfews. Many framed Covid-19 as a security threat not just a public health issue. As argued by scholars of the Copenhagen School this move has definitive political consequences, as "securitization is a political choice by policy makers and not a "natural" state (Hoffman, 2020). The securitization of disease is dangerous as it gives additional powers to governments to suspend fundamental citizenship rights and has led to the militarization of responses in some countries. It creates tools and modalities for future repression and is especially dangerous in contexts with insufficient legal safeguards and social safety nets (Lynch, 2020). The introduction of Covid-19 tracking apps is one vivid example of how governments can legitimately use state control to gather personal information from their citizens, which is questionable in terms of both ethics and privacy (Rolland, 2020).

In March 2020, the UN High Commissioner for Human Rights issued a statement noting: "the use of emergency powers must be publicly declared and should be notified to the relevant treaty bodies when fundamental rights including movement, family life and assembly are being significantly limited" (United Nations, 2020). However, as many scholars argue, once emergency laws are put in place, they are unlikely to change, especially in oppressive state regimes. As Hoffman notes: "The lessons about the ability to clear the streets, the technology to track citizen movements, the legal authorities to implement lockdowns – all of these are equally useful against political opponents as they are against the virus" (Hoffman, 2020).

Methodology

The methodology utilized here consists of first, a technical assessment of Covid-19 apps available in the four regions and second, 10 case studies of countries that introduced apps as part of their public health response. For the first stage, technical criteria with potential implications for privacy were identified; every developed app was examined based on their publicized features, the existence of privacy laws and of data protection authorities. In the second stage, nine countries

were analyzed considering: data protection and the privacy environment; the adoption of Covid-19 apps as a public health measure; evidence of "function creep" or data misappropriation; and potential impact on human rights of vulnerable populations. Given the novelty of these developments, the majority of the data was obtained through secondary sources and "grey" literature, though some academic sources were included. In order to supplement the absence of evidence on specific criteria – particularly function creep and effects on vulnerable populations –, two interviews with members of civil society are included.

AFRICA

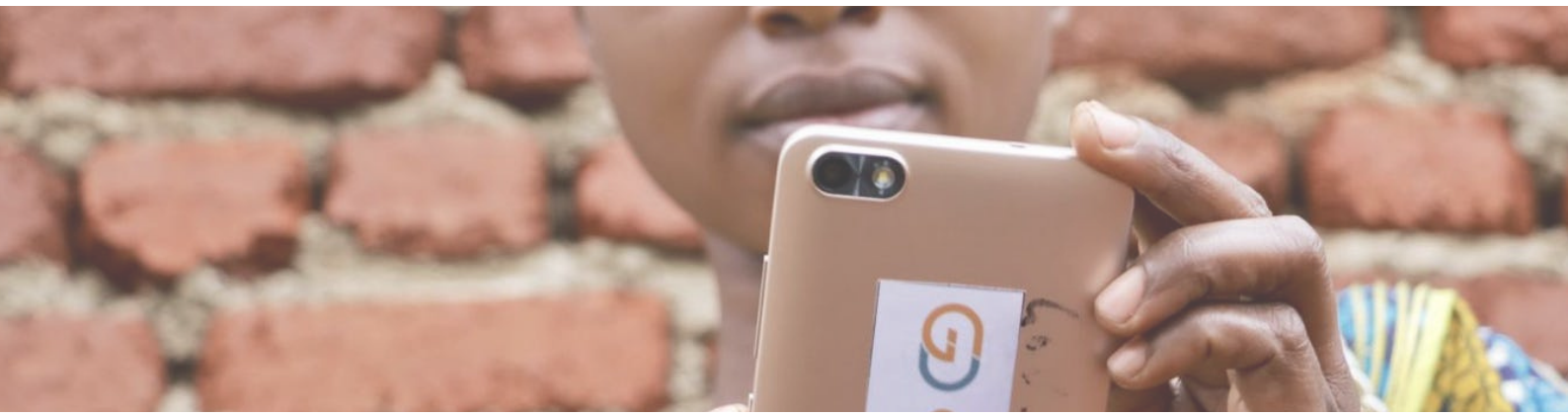


Image source: WHO

Africa

I. Covid-19 Apps

Of the 54 countries in Africa, 21 (39%) have developed Covid-19 apps. However, only 11 (20%) have developed Covid-19 apps that include contact tracing elements. These countries are Algeria, Botswana, Cape Verde, Egypt, Ethiopia, Ghana, Kenya, Morocco, South Africa, Togo, and Tunisia. Since four of these countries (Algeria, Egypt, Morocco, and Tunisia) are considered part of the Middle East and North Africa (MENA) region, when considering sub-Saharan Africa, 7 out of 46 countries (15%) have developed Covid-19 apps including contact tracing (see Appendix 1). This represents a lower presence of Covid-19 contact tracing apps in sub-Saharan Africa countries compared to the Middle East (79%), Southeast Asia (64%) and Latin America (63%).

Three of the Covid-19 apps (14%) have a stated mandatory component: Kenya's mSafari app requires that those taking public transport including buses and taxis register for contact tracing and Seychelles 'and Togo's apps are mandatory for those traveling to the countries. Among these, the Kenyan and Togo apps use contact tracing.

The apps in the region that do not include contact tracing focus predominantly on Covid-19 education, case statistics, and self-diagnosis tools.

Several of the apps have linked privacy policies that are incomplete or link to a generic government page. Notably, the Moroccan app does not have any privacy policy while Egypt's privacy policy links to an unresponsive page. Cape Verde's privacy policy links to a generic government coronavirus response page and Ethiopia's Debo app links to a limited privacy policy.

II. Privacy, Data Protection and Human Rights

Data privacy in Africa is still nascent and under development. Of the 54 African countries, 29 (54%) have Data Protection and Privacy Legislation in place, 9 (17%) have Draft Legislation, 12

(22%) have no legislation, and 4 (7%) have no data (United Nations Conference on Trade and Development, 2020). However, despite over half the countries having data protection laws in place, many do not have appropriate data protection authorities (DPA) to enforce them (Illori, 2020). Some of the key data protection challenges include: a lack of independence of DPAs from local government; limited funding and regulation to ensure data protection rights; lack of institutional capacity to create or manage data protection laws; duplication of data collection by multiple departments; and low law quality (Illori, 2020). There have been discussions and draft regional Privacy Legislation, such as the proposed Malabo Convention, which would create data rights and encourages countries to establish their own data protection policies, but there is currently no enforced regional protection covering the entire continent or portions of it (Illori, 2020; Razzano, 2020).

Specific to Covid-19, one of the data privacy challenges has been the state of emergency that enables potential restriction of privacy rights: 45 African countries have introduced Covid-19 legislation, 37 have imposed human rights limitations, and 18 have declared states of emergency, but only 7 of these nations have existing and enforced data protection laws (Illori, 2020).

III. Case studies

Ghana

Ghana enacted a Data Protection Act & Data Protection Commission in 2012, which regulates how personal data is acquired, retained and disclosed. The country also established a Data Protection Commission to ensure enforcement of the laws (Parliament of the Republic of Ghana, 2012). In March 2020, the Ghanaian government passed Executive Instrument (EI) 63, which gives the state power over telecommunication systems in a public emergency (Oduro-Marfo, 2020). This requires Mobile Network Operators (MNOs) to allow the state to access their networks and enables a database linking individuals to their phone numbers and phone models (ibid.). This new instrument is exempt from the existing Data Protection Act, due to its nature as a national security, public safety and emergency measure (ibid.). Although the EI has been challenged in court because

it covers public emergencies broadly and does not have an end date, it has been legally upheld in court (Oduro-Marfo, 2020; Dzawu, 2020). Critics have highlighted the potential for ongoing surveillance and intervention once the Covid-19 pandemic ends (Oduro-Marfo, 2020).

A public/private data collaboration initiative between the government and an MNO, Vodafone, was initially established in 2018, and has been leveraged to address the Covid-19 pandemic (SDSN TReNDS, 2020). The collaboration between the Ghana Statistical Service (GSS), Vodafone Ghana, and an NGO, Flowminder, enabled GSS access to mobile data for public health and development (ibid.). This collaboration included a formal agreement between the parties as well as with the Data Protection Commission and Ghana National Communications Authority which established data anonymization and aggregation, data handling restrictions, data use limitations, and data deletion clauses (ibid.). This agreement has enabled GSS to analyze the impact of population movement restrictions during Covid-19, including monitoring the movement of active mobile subscribers across regions (SDSN TReNDS, 2020; Burns, 2020).

COVID-19 App: GH COVID-19 Tracker

Ghana launched its Covid-19 app, "GH COVID-19 Tracker", in April 2020. The reported capabilities of the app include: checking symptoms against WHO criteria; monitoring self-quarantine; tracking area updates and hotspots within a 1 km radius; registering event attendance or checking in at a venue; and helping authorities to trace and inform individuals in the event of an outbreak (Ghana Ministry of Communications, 2020). Despite some public concerns about personal data collection, the Ghanaian Communications Minister, Ursula Osusu-Eduful, has reassured the country that personal data is not collected and the government only has locations and phone numbers, not individual names, in line with EI 63 (ITU News, 2020). The app's privacy policy aligns with the 2012 Data Protection Act, including assuring that data is only used for its designated purpose, that data is only retained for the necessary amount of time, although it may be shared with the "Commission's controlled affiliates" when necessary to protect lives (Ghana Data Protection Commission, 2020). The app's privacy policy includes user consent to utilize data, although a study that included the GH COVID-19 Tracker and evaluated the readability of privacy policies for Covid-19 apps found that these policies require a reading level between grades seven

and fourteen, which is higher than the reading level of the average user (Zhang et al., 2020). The GH COVID-19 Tracker app is one part of Ghana's Covid-19 response, which also includes social distancing measures, travel and border restrictions, partial lockdown, drones for Covid-19 test sample collection across the country, building new infectious disease centers, and incentives for healthcare workers (Zhang et al., 2020).

Kenya

The Kenyan constitution has privacy guarantees and a Data Protection Act (DPA) that was signed in late 2019 (Mutung'u, 2020). The Act established the Office of the Data Protection Commissioner, introduced personal data protection rights, created grounds for processing sensitive data, and regulated the transfer of data within and outside of Kenya (Republic of Kenya, 2019). Critics, however, argue that the act is not operationalized and that the Kenyan court has increasingly enabled technology with limited privacy restrictions (Mutung'u, 2020). According to an interview with a Kenyan data privacy lawyer (known as Lawyer from here on), while the Data Protection Act was signed in 2019, the Commissioner was only added in late 2020 and the website launched in early 2021, which raises concerns around data privacy and protection (Lawyer, 2021).

COVID-19 App: mSafari

In response to Covid-19, Kenya launched "mSafari" in March 2020. This app requires public transport passengers to register their contact details through their phones in order to make a cashless payment for their trip, (WHO, 2020). Passenger manifests are then shared with the Kenyan Ministry of Health for contact tracing (ibid.). The app is required for all public service vehicle (PSV) operators and passengers, including buses, taxis, and motorbikes, and mSafari enables GPS tracking for vehicles (INCLO, 2020; EIB, 2020; Access Now, 2020). According to the Lawyer, this has not actually been implemented as a mandatory practice (Lawyer, 2021). However, as an estimated 50% of the Kenyan population uses PSVs on a daily basis (EIB, 2020), especially those who are lower income, this registration policy has a greater impact on vulnerable lower income populations (Lawyer, 2021). The Kenyan Human Rights Commission has raised concerns

that a clause within the DPA exempts privacy and data protection for data being processed for national security or public order (INCLO, 2020). Additionally, according to the Lawyer, these data have been stored in central servers which have been hacked in the past (Lawyer, 2021). There is also a precedent of similar data being used for political purposes or counter-terrorism efforts (Mutung'u, 2020; Nkatha, 2020).

In January 2021, Kenya became the first country to adopt the Trusted Travel program, which was developed as a public-private partnership with PanaBIOS[2], Econet[3], the African Union, and Africa CDC[4], and enables travelers to upload Covid-19 test results for travel authorization, including information on country entry/exit requirements (Harrison, 2021). As of January 11, 2021, all travelers entering or departing Kenya are required to show a digitally verified negative Covid-19 test via the Trusted Travel PanaBIOS app (Overseas Security Advisory Council, 2021). The app was designed for use across Africa; however, Kenya is the first country to adopt it. As highlighted by the Lawyer, this could present a risk when entering a country with different or limited data privacy laws (Lawyer, 2021). The app uses blockchain technology to store information securely and provides a digital record to ensure against counterfeit or fake tests (New African, 2020). The PanaBIOS app also has digital contact tracing capabilities, relying on uploaded health records to identify hotspots, although the app does not have GPS or Bluetooth enabled contact tracing at this stage (PanaBIOS, 2021).

In addition, the Kenyan government has monitored quarantine compliance through mobile phone tracking, including geo-location (Access Now, 2020). While this is typically only allowed with a warrant, the emergency nature of Covid-19 has made this practice permissible (Monyango, 2020). Other technology solutions have been incorporated into Kenya's Covid-19 response including mobile money transfer solutions (Mutung'u, 2020). These initiatives help to manage the pandemic, but cause concern given the lack of clarity about the nature of these initiatives and the policies governing them (ibid.).

[2] A digital application built by African technologists for disease monitoring, testing, and tracking
[3] A private telecommunications company based in South Africa
[4] Africa Centres for Disease Control and Prevention

IV. Conclusion and Recommendations

The technological solutions created because of the Covid-19 pandemic have raised concerns around data privacy in Africa. The limited number of data protection laws and authorities in place across the region (Illori, 2020) lead to transparency concerns around how data is used and shared. Many countries do not enforce their data protection laws, leaving citizens with no means of support should their data be misused. As well, draft regional reforms such as the Malabo Convention have yet to be ratified (ibid). As a consequence, the following guidelines are recommended.

- Accountability: Establish regional and country-specific data protection laws to hold governments and companies accountable for how data are used. Establish Data Protection Authorities to enforce laws and introduce legal support in the event of data misuse.
- Transparency: Ensure that app functionality, data use and timeframe, and data storage location are all explicitly shared.

LATIN AMERICA

Image source:Americas Quarterly

Latin America

I. Covid-19 Apps

Fifteen countries in the region have developed Covid-19 apps. Nine of them have privacy laws: Argentina, Brazil, Chile, Colombia, Costa Rica, Dominican Republic, Mexico, Peru, and Uruguay. Countries that developed an app without having specialized legislation are Belize, Bolivia, Ecuador, Guatemala, Panama and Paraguay. Of the 15 apps, only 9 provide a privacy policy on the download page. Only in Argentina was the app mandatory for people going back to work and entering the country. In most countries, the app developer is either the Ministry of Health or the E-Government national agency. Only the developers of the Guatemalan and Argentinean apps are private technology companies, though they partnered with the government. Only eight have contact tracing among their functionalities; however, 11 have GPS among its permissions, and six allow the use of Bluetooth (see Appendix 2).

Jamila Venturini, regional coordinator of the civil society organization Derechos Digitales observed that half the apps met all consent requirements, but several inconsistencies were found regarding consent requests and data collection practices. Due to low-capacities for epidemiological monitoring, some governments suggested that the data collected would be useful for this purpose; nevertheless, informing public health measures with data gathered by apps poses the risk of misinformed interventions (Venturini, 2021). Venturini also observed that in the context of emergency, privacy rights were relativized, allowing the use of data for statistical and public health purposes, which could be considered as a "hidden functionality" of some apps.

II. Privacy, Data Protection and Human Rights

Civil liberties are widely covered in regional legislation; however, the region lacks a unified framework that protects personal data (Mendel and UNESCO Office Quito and Regional Bureau

for Communication and Information in Latin America and the Caribbean, 2009). The regional guideline for data protection is the EU General Data Protection Regulation (GDPR). Before 2018, most countries had national legislation that regulated privacy and data protection; nevertheless, the adoption of the GDPR forced local policies to adjust to EU standards through developing more specialized and protective laws. Among the new reforms, concepts such as biometric data and "the cloud" were introduced, national data protection authorities were created, and more stringent fines were established (Bojali and Vela-Treviño, 2019). Of the 25 countries in the region, 10 have specialized privacy laws (41.6%), of which 8 have a data protection authority (DPA). However, enforcement of privacy laws remains low, partly due to the developing stage of DPAs in some countries and their absence in others (The Bureau of National Affairs, 2015). Countries with relatively well-functioning DPAs are Colombia, Mexico and Peru (The Bureau of National Affairs, 2015), whereas Chile and Dominican Republic do not have a DPA. Venturini indicated that surveillance and high variation in degrees of data protection across countries characterize data rights in Latin America (Venturini, 2021).

III. Case Studies

Guatemala

Even though the Guatemalan constitution includes freedoms of expression and access to information, the Personal Data Protection Law still remains an initiative (OAS, 2021) which means the Access to Public Information Law regulates personal data issues (Fratti, 2019). Guatemala has precedents of serious cybersecurity violations by the government: in 2018, it was discovered that such operations are carried out against businessmen, politicians, journalists, diplomats and activists (Nuestro Diario, 2018). This raises concerns about increased susceptibility to surveillance for some groups.

COVID-19 App: Alerta Guate

"Alerta Guate" was launched on March 29, 2020 by the Guatemalan government as an emergency communication service, whose primary goal was to provide citizens with public health information. The app was funded by Tenlot, a multinational company that runs the lottery in Guatemala and it was developed by In-telligent LLC, which held the gathered data (Global Witness, 2020). The app was removed from Apple and Android app stores in April after civil society organizations pointed out that the privacy policy stated that access to geolocation is permitted, data can be used for advertisement purposes and personal information could be shared with third parties (In-telligent, 2020). The president of Guatemala suggested the app could be used to contact the national police directly and pointed at the possibility of using it for security purposes (Méndez, 2020). Concerns were also raised by the fact that the funding company used it to advertise lottery tickets (Global Witness, 2020).

Uruguay

Uruguay has advanced data protection governance. Data rights are regulated by the Protection of Personal Data Law Nº 18331 and the Habeas Data Action 2008 Decree; the corresponding regulator is the Uruguayan Data Protection Authority (Brian-Nougrères, 2020). In April 2020, Telemedicine Law No. 19,869 was approved and set regulations for health provision through information and communication technologies. The law provides that information produced by telemedicine is considered sensitive, as established by the Personal Data Protection Law, meaning that security and confidentiality measures need to be guaranteed (Centro de Información Oficial, 2020). Finally, another element of Uruguay's digital environment is its electronic governance agency, AGESIC, which was created in 2005 with the purpose of promoting access to information, and inclusion related to information and communication technologies.

Covid-19 App: CoronavirusUY

The "CoronavirusUY" app was launched by the Uruguayan Ministry of Public Health in collaboration with the private investor ThalesLab, and software developer Genexus, and operated

by AGESIC and the Ministry of Public Health (IDB, 2020). Its main features are communications – including telemedicine – and contact tracing (Milano, 2020b). Telemedicine functionalities allow patients to communicate with their doctors through messages or videocalls, enabling real-time healthcare monitoring (IDB, 2020). The app also enabled a function that allows foreigners to submit their PCR test before entering the country (Milano, 2020a). Concerns were raised around the early adoption of Google and Apple's contact tracing protocol (Scrollini et al., 2020), given the absence of clear criteria on how information was to be shared. This poses a potential increased risk for data generated by telemedicine, which is considered sensitive according to data protection regulations. Even though Google and Apple's data-sharing procedures became more transparent as a result of the supervision from AGESIC and scholars (Kaminer and Pagola, 2021), there have been demands from scholars and civil society members for further data governance guidelines (Scrollini et al., 2020).

Argentina

Argentina has a data protection framework, the Personal Data Protection Law 253226, and an enforcing organism, the Agency for Access to Public Information (AAIP). In March, the AAIP issued a statement providing that Covid-19-related data is considered sensitive and the object of more rigorous protection (Ministerio de Justicia y Derechos Humanos Presidencia de la Nación, 2000). Among the new guidelines, disclosure of Covid-19-related information requires the patients' consent, especially for purposes other than medical treatment. However, it also authorizes the Ministry of Health and provincial ministries to require, collect and process health-related information without patients' consent (Agencia de Acceso a la Información Pública, 2020).

COVID-19 App: Cuidar

The "Cuidar" app was developed by the Public Innovation Secretariat, the Ministry of Science and Technology, the Sadosky Foundation, the National Council of Scientific and Technical Research, and the Chamber of Software Industry. Data is stored on the Amazon server in the US (Clarín, 2020). Its main publicized functionalities are self-diagnosis and the generation of a

circulation permit. The user must provide personal data, mobile number, and address, and is required to activate geolocation on their phones. Also, users must provide information such as body temperature, symptoms and pre-existing health conditions if they want to self-diagnose (Ámbito, 2020). Data regarding diagnosis is centralized and managed by Provincial Emergency Committees, which are in charge of providing health recommendations to infected persons. The app's webpage indicates that only these committees are allowed to monitor data on users' symptoms (Gobierno de Argentina, 2020). The use of the app was mandatory for those who returned to work (La Nación, 2020), and users entering the country are required to have it installed for at least 14 days (El Cronista, 2020). When citizens complained about the possibility of permanent location surveillance, this functionality was modified to allow geolocation only when the app is in use (Clarín, 2020). Amnesty International suggested that requiring people to self-diagnose in order to get a circulation permit was unnecessary, raising concerns about the lack of transparency regarding the way data is treated and secured and pointing out that people with no access to digital technology were potentially excluded from acquiring circulation permits (Amnesty International, 2020).

IV. Impact on the human rights of vulnerable populations

Even though there is no evidence of social control on vulnerable populations in the region, the potential to exclude some individuals from certain services and the constraints to free transit are matters of concern. Our informant pointed out that when the app was mandatory, some groups had access difficulties, specifically those without official documents, posing limitations to their ability to access social rights and circulation permits. In this way, access to transit can be constrained among certain populations when the app was a requirement to access certain places, for instance, going back to work as was the case in Argentina (Venturini, 2021).

V. Conclusion and Recommendations

Contact tracing apps raised the need to improve data protection regulations and enforcement, even in countries with well-developed legal frameworks. Even though there is no evidence of surveillance in the region, several challenges regarding accountability and transparency need to be addressed. Also, the role of apps as containment measures needs to be evaluated from a public health perspective, not only through a technological lens. Policy improvements should be undertaken in three key areas: transparency, accountability and proportionality.

- Improve transparency in regard to gathering, storage and use of data. The purpose of data collection needs to be clearly stated and subject to consent standards.
- Strengthen the clarification in most apps privacy policies regarding the degrees and conditions of access to data by public and private entities (Venturini, 2021). Public-private partnerships should operate in accordance with legal frameworks.
- Create spaces for public debate and participation of civil society and scholars in designing, implementing and evaluating apps.
- Conduct thorough proportionality evaluations. Granting permissions requires justifications that balance their contribution to outbreak control with potential human rights costs.

SOUTHEAST ASIA

Image source: Innovation Village

Southeast Asia

The South East Asian (SEA) region includes the following 11 countries: Brunei, Cambodia, East Timor, Indonesia, Laos, Malaysia, Myanmar, the Philippines, Singapore, Thailand and Vietnam. Most countries have responded to the Covid-19 crisis with emergency legislation, increased surveillance, suspension of democratic activities and movement flows, introduction of social distancing measures, lockdowns, and curfews. To monitor the spread of the disease, governments have introduced contact tracing applications that can be downloaded to smartphones and tablets. While the effectiveness of digital surveillance is disputed, concerns have also been raised about the potential erosion of privacy and human rights.

I. Covid-19 Apps

Of the 11 SEA countries, 9 (81%) have developed Covid-19 applications, with the exception of Cambodia and East Timor.

Brunei's "BruHealth" contact tracing app was developed by the E-Government National Center in collaboration with the government's Ministry of Health, and it must be used when entering all business premises. Its system is centralized, which means that the data is stored in the government's server. Its privacy policy is available online.

"Peduli Lindungi" was developed by the Indonesian Ministry of Communication and Information Technology. Its privacy policy is not available in English and its system is centralized.

The "LaoKYC" app in Laos was developed by a private telecommunications company called SB Lab 856 Co, Ltd in collaboration with the Ministry of Posts and Telecommunications. It uses Sim card registration to track potential Covid-19 positive cases, but, according to its permissions, strangely enough, it does not use Bluetooth for tracing. Its privacy policy is available, and the system is centralized.

Malaysia has seen the development of a multitude of applications: “MySejahtera”, “MyTrace”, and Gerak Malaysia. The latter was only used as a beta test and has been discontinued and its data destroyed (Asia Centre 2020). Developed by the Malaysian government for the Ministry of Health, MySejahtera aims to inform the population about the evolution of the crisis. MyTrace is a contact tracing application, developed by the International Islamic University Malaysia and Google Malaysia, and authorized by the Ministry of Science, Technology and Innovation. Both apps are centralized and have accessible privacy policies.

Myanmar’s contact tracing app, “Saw Shar”, was developed by the Myanmar Computer Federation for the Coronavirus Disease 2019 Control and Emergency Response Team in collaboration with the Ministry of Transport and Communication and the Ministry of Health and Sport. However, it has been a cause for concern recently, as there have been reports of a cyberattack on its database, which unfortunately is not decentralized.

In the Philippines, the “StaySafe” contact tracing application was developed by a private company, Multisys Technologies Corporation, and licensed by the Department of Health. It has drawn some criticism because it was developed privately, particularly with regard to data use transparency, as there are numerous permissions required. This case will be discussed further below.

The Singapore Government Technology Agency developed “TraceTogether”, a contact tracing application, and “SafeEntry”, a national registration system mandatory for entering business premises. TraceTogether has a decentralized system, which means that the data collected is encrypted and only reported to the Ministry of Health in an anonymized manner if the user tests positive for Covid-19. SafeEntry has a centralized system.

Thailand also has two applications: one contact tracing app, “ThaiChana”, and another to provide information to health professionals, “MorChana”. The first was developed by Krung Thai Bank and licensed by the government. The second was developed by the Digital Government Development Agency, but has been widely criticized because its permissions require access to the user’s application history and location, which means that the government could access data unrelated to Covid-19.

The Vietnamese Ministry of Information and Communications and the Ministry of Health have authorized “Bluezone”, a contact tracing application developed by Bkav, a cybersecurity technology company. The application uses a decentralized system. This case will also be discussed later on.

Overall, of the 12 applications reviewed, 83% (10) have a centralized system, meaning that all data collected is stored in government/company databases, 58% (7) were developed by a government entity and 75% (9) have an accessible privacy policy. This raises clear concerns about practices and regulations regarding how data is stored, gathered, used and mostly importantly protected (see Appendix 3).

II. Privacy, Data Protection and Human Rights

In November 2016, the Association of Southeast Asian Nations (ASEAN) adopted a Framework on Personal Data Protection, which established a set of national and regional principles to promote and strengthen personal data protection (Deloitte, 2018).

Malaysia, Singapore, the Philippines and Thailand implemented Personal Data Protection Acts (PPDAs) in 2010, 2012s and 2019 respectively, which are enforced by PPD Commissions. These laws require that citizens be informed, give consent and understand why and when their data is collected and that they are allowed to access the information stored. They prohibit any disclosure of data without consent and require that data be kept securely for a period defined in the privacy policies before being destroyed. In Thailand, the pandemic has slowed down the law’s implementation and some companies have been granted an extension of the compliance deadline until June 2021, which could become an issue since Thailand’s contact tracing application was developed by a private company.

Brunei, Indonesia, Laos, Myanmar and Vietnam do not have PPDAs. Data protection is addressed in other laws such as the Indonesian Ministry of Information and Communication Regulation No.20/2016, the Lao Laws on Protection of Electronic Data (2017) and Cyber Crime (2015), and the Vietnamese Laws on Cyber Information Security (2016) and Information Technology (2006). The government of Brunei issued a data protection policy in 2014, but it only

covers data held by government entities, not by private companies. Myanmar issued a law in 2017 entitled Protecting the Privacy and Security of Citizens, which outlaws the interception of citizens' electronic communications unless warranted by an order.

Overall, while there is a regional legal framework on data privacy in the SEA region, there is a clear disparity between countries. While the more developed countries have adopted PPDAs that are enforced by commissions, the less developed half do not have PPDAs and only address data protection via other laws.

III. Case Studies

We chose two case studies, StaySafe in the Philippines and Bluezone in Vietnam, because they are different from each other in terms of app configuration and data protection laws. Although both were developed by private companies and authorized by government entities, Bluezone has a decentralized system and does not have a PPDA to comply with, while StaySafe has a centralized system and must comply with a PPDA.

The Philippines

The Philippine PPDA was issued in 2012 and was implemented in 2016 with the creation of the National Privacy Commission.

COVID-19 App: StaySafe

The StaySafe application was developed by a private company, Multisys Technologies Corporation, and licensed by the Department of Health. It has three objectives: health status reporting, social distancing, and contact tracing. Its system is centralized, which means that the data is stored in the developer's centers. StaySafe's development by a private company has led to some criticism, particularly regarding data transparency given the high number of permissions it requires (Mendoza, 2020). Further, the permissions do not specify whether the application has access to GPS and/or Bluetooth which would enable effective contact tracing. In addition, while a

national task force is supposed to monitor the data collected by the application, a lack of accountability was noted by the Asia Centre (2020). Its report notes that the task force is comprised of multiple government entities, which increases the risk that citizens' private data could be shared without any control or restriction. This is of particular concern in relation to data protection and human rights.

Vietnam

Vietnam does not have a PPDA, but some of its laws address data privacy, such as the laws on Cybersecurity (2016), Information Technology (2006), Electronic Transactions (2005) and Protection of Consumer Rights (2010). Article 21 of the latter requires an individual's consent prior to any collection and use of data, in addition to a required notice to explain why the data is collected and the individual's right to manage their data.

COVID-19 App: Bluezone

The Vietnamese contact tracing application, Bluezone, was developed by Bkav, a technology company specializing in cyber security and licensed by the Ministry of Information and Communications and the Ministry of Health. The application uses a decentralized system, which means that information is stored on the user's device and is set up to notify the user if there has been close contact with someone diagnosed with Covid-19. The application has been applauded for many reasons. First, it is, along with Singapore's app, one of the applications that requires the fewest permissions to perform contact tracing functions (Shepherdson, 2020). Second, it is one of only two apps with a decentralized system and therefore limited data collection. Yet, a Vietnamese security engineer noted that the application is still "capable of harvesting information, which could be used by authorities to track interaction between people" (Kim, 2020).

IV. Impact on the human rights of vulnerable populations

While the pandemic and its effects are only just beginning to be assessed and reported, some NGOs have already written reports on the increased control of governments over individual rights in SEA. Increased digital surveillance is a hotly debated topic, particularly in view of its potential to violate human rights and data protection under the guise of health measures. Data may be manipulated to allow the arrest of anti-government and pro-democracy activists under the pretense of public health.

The Asia Centre's report on Covid-19 and Democracy in Southeast Asia (2020) highlights the early effects of increased digital surveillance, particularly on women and youth, who have recently become the new faces of resistance in the region.

The Institute for Internet and Just Society recently published a report on the Philippines which concluded that limitations on freedom of movement have enabled abuses and human rights violations such as the case of three young LGBTQIA+ people who were interrogated for violating curfew and accused of seeking illicit sex. They were publicly humiliated as punishment: ordered to kiss, dance and do push-ups on a live video broadcast on social media (Baysa-Barredo, 2020).

V. Conclusion and Recommendations

Crisis literature highlights how past restrictions can turn into long-term laws and policies that erode democratic institutions and reduce civic space. From the Asian financial crisis of 1997 to the Covid-19 pandemic in 2020, the SEA region has experienced a crisis that has increased authoritarianism and statism, negatively impacting democracy and human rights.

To limit the impacts of digital surveillance on human rights and data protection in SEA, several actors need to be involved.

The United Nations

- Must enable greater civil society participation in multilateral discussions.

- Need to apply the M&E mechanisms from the Universal Periodic Review (UPR) to ensure that states' accountability.

SEA governments

- Should be pressured to dismantle emergency laws and contact tracing applications.
- Should be compelled to comply with the standards of international human rights treaties.
- Should strengthen their collaboration with civil society organizations (CSOs) that promote democracy and human rights.

Local, national and international CSOs and NGOs

- Should be empowered to build resilience, ensure government accountability and counter authoritarianism.
- Should be supported in their collaboration with multilateral platforms and governments.

MIDDLE EAST

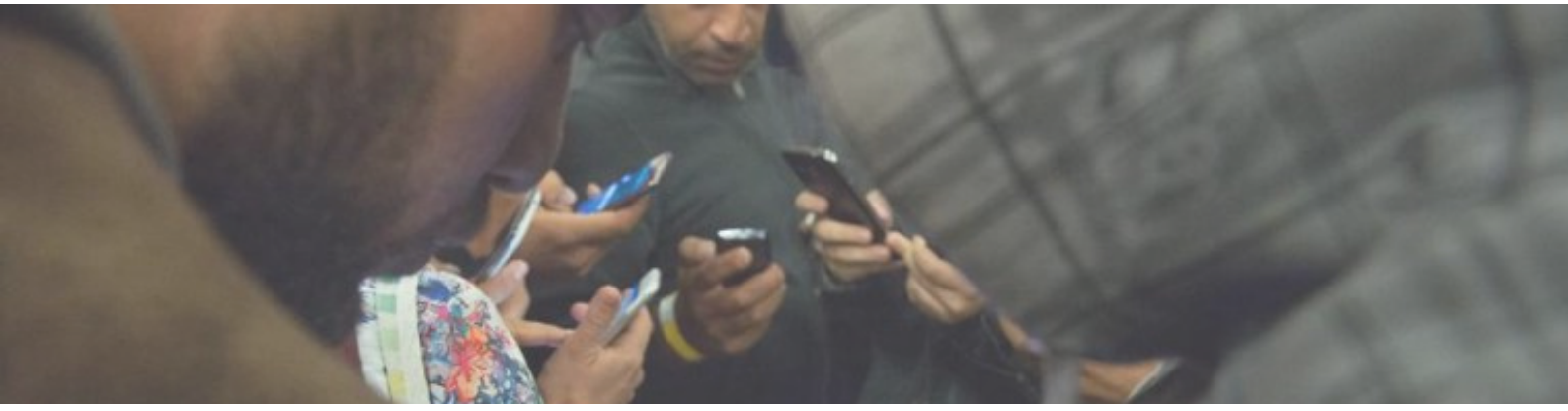


Image source: BBC

Middle East

The Middle East and North Africa region (MENA) includes the following 19 countries: Algeria, Bahrain, Egypt, Iran, Iraq, Israel, Jordan, Kuwait, Lebanon, Libya, Morocco, Oman, Qatar, Saudi Arabia, Syria, Tunisia, United Arab Emirates, Palestine, and Yemen. The majority of these countries developed policy and technological solutions to halt the spread of Covid-19 virus, including declaring a state of emergency, closing borders, restricting movements, and introducing social distancing measures and nighttime curfews. As of March 2021, all 19 countries made the use of masks mandatory in public venues and public transportation. Fifteen of the 19 countries require Covid-19 tests for incoming passengers, some require mandatory quarantine. All countries introduced a variety of lockdown measures, with full lockdown, partial lockdown, or a nighttime curfew in place at the time of writing this report (Organisation for Economic Cooperation and Development, 2020).

The majority of countries also introduced technological solutions to halt the spread of the virus. While contact tracing apps are an important means to track and contain the virus, as Human Rights Watch stated these apps "whose utility in controlling the pandemic has yet to be proven, may introduce unnecessary and disproportionate surveillance measures in public health disguise" (Human Rights Watch , 2020). This holds especially true in countries with a poor human rights track record, in particular the Middle East, where governments heavily restrict freedom of expression and civil society activities, and persecute those criticizing the authorities on social media. Hundreds of human rights defenders were targeted in 2019 alone (Amnesty International, 2019).

In April 2020, 110 organizations in the MENA region issued a statement calling upon the governments to ensure that the pandemic not be used as a pretext to deploy digital surveillance measures: "Technology can and should play an important role during this effort to save lives…, however, an increase in state digital surveillance powers, such as obtaining access to mobile phone location data, threatens privacy, freedom of expression and freedom of association, in ways that

could violate rights and degrade trust in public authorities…" (The Tahrir Institute for Middle East Policy, 2020).

I. Covid-19 Apps

Of the 19 MENA countries, 15 (79%) countries have developed Covid-19 contact tracing applications (see Appendix 4) while Iraq, Syria, Palestine, and Yemen have not. In most countries, the apps were developed by the Ministry of Healthcare or the equivalent government agency. In Algeria, Jordan and Tunis, the applications were created by tech start-ups. In Lebanon, the app was designed by professors and students at the American University in Beirut. In all cases the applications were authorized by the Ministry of Healthcare.

Some of the common features of the apps, as described on the Google Play or Apple Play Stores, include providing the latest health updates, educating the public on the measures to combat the virus, contact tracing and communicating with the healthcare authorities. For example, a Health Bot in the case of Kuwait is able to diagnose the possibility of having contracted the virus by asking Yes/No questions.

While most of the apps are voluntary, Bahrain, Qatar and Kuwait rolled out some of the most invasive applications mandating self-isolating individuals to use the contact tracing app and "carrying out live or near-live tracking of users' locations by frequently uploading GPS coordinates to a central server", sparking criticism by international human rights organizations that governments were putting the privacy and security of hundreds of thousands of people at risk (Amnesty International, 2020).

Most of the apps use both GPS and Bluetooth systems for contact tracing. All apps seek access to other features of the phone besides location service, such as device/app history, microphone, camera, contact and photo/media files. Ten out of 15 apps has their privacy policy indicated on the Google and/or Apple Play Stores. "Egypt Health" of Egypt, "Speetar" of Libya, and "WIQAYTNA" of Morocco do not have a privacy policy section. While Kuwait's "Sklonik" includes its privacy policy, the website is inaccessible. Iran's "AC19" and "Mask" apps were removed from both Google Play and Apple Play Stores in the summer of 2020. The number of app downloads

varies from country to country, from one million+ in Israel, Morocco and Qatar to five thousand+ in Libya.

II. Privacy, Data Protection and Human Rights

Data privacy frameworks in the MENA region are very recent and complex. Most of the privacy provisions were formerly provided under different legislative frameworks, such as the constitution and civil code, rather than in specific laws on data protection. However, the EU's 2018 General Data Protection Regulation (GDPR) spurred the creation and revision of privacy laws around the world, including in the Middle East (GSMA, 2019). Since 2018 many MENA countries either updated their existing legislative frameworks to reflect the GDPR or created the new data privacy laws. The following eight (42%) have enacted data privacy legislation: Algeria, Bahrain, Egypt, Israel, Lebanon, Morocco, Qatar and Tunisia. Egypt being the latest, adopting the Data Protection Law in July 2020, with full enforcement delayed until 2022.

United Arab Emirates, Saudi Arabia and Kuwait do not have specific data protection laws, although their Cyber Crime and Electronic Transactions legislation provide limited data protection. In Saudi Arabia, where Sharia principles are the primary source of the law, a new freedom of information and protection of private data law is under review by the formal advisory council of the Kingdom of Saudi Arabia (DLA Piper, 2021). Whilst Oman's Constitution (Royal Decree No. 101 of 96) recognizes an individual's right to confidentiality in all forms of communication, it does not recognize the right to privacy as a fundamental right beyond this (PWC, 2021). The data privacy laws in the rest of the region are either very general, scattered through different legislations or non-existent.

While creating data protection frameworks is a positive step toward recognizing privacy, the primary challenge is how to enforce the laws effectively. Algeria, Bahrain, Israel, Morocco, and Tunisia have set up Data Protection Authorities. In Qatar, the Ministry of Transport and Communications is responsible for implementing and enforcing the law, while Lebanon has failed to create an independent regulatory body altogether. Even in the countries with allegedly

independent Data Protection Authorities, personal data has been breached and personal information misused.

There is no regional framework of data privacy in the Middle East region.

III. Case Studies

Bahrain

Bahrain was one of the first Arab nations to adopt Personal Data Protection Law (Law No 30) in 2018. The law is consistent with international practices and is rooted in the GDPR. It includes protection of individuals' privacy and includes specific consent requirements for data protection.

The law applies to natural and legal persons residing or working in Bahrain as well as those individual or legal persons who process data using the means that exist in Bahrain. Article 3 of the Data Protection Law defines the principles of how data should be collected, stored and used (GSMA, 2019).

Bahrain also has a number of other provisions related to data security, including the constitution, the Penal Code (Amiri Decree No 15 of 1976), the E-Transactions Law (Legislative Decree No 54 of 2018), the Telecommunications Law (Legislative Decree No 48 of 2002) and the Cyber Crimes Law (Law No 60 of 2014) (ibid.). However, these laws do not apply to data processing carried out in personal or family matters, neither does it apply to operations related to national security issues, Ministry of Defense, Ministry of Interior, the National Guard, the National Security Services and other security services (SMEX, 2021).

To ensure that the laws are enforced and implemented, the law stipulates the creation of the Personal Data Protection (PDP) Authority; however, this body is yet to be set up. Currently, the Ministry of Justice and Islamic Affairs and Endowments exercises this role (Ali, n.d.).

The creation of the PDP law was directly influenced by the country's ambitious plan to become a hub for data centers which led to Amazon Web Services opening its first Middle East center in Bahrain in 2019.

COVID-19 App: BeAware

The government of Bahrain requires self-isolating individuals and people arriving in the country to download the "BeAware" app. The app is paired with a Bluetooth bracelet to notify the authorities if a person leaves their household. It is mandatory for individuals who are registered for home quarantine to wear the bracelet and those who remove it can face legal penalty under the Public Health Law No. 34 (2018), imprisonment of at least 3 months and legal penalty between BD1,000 and BD10,000 (approximately USD2,700, and USD27,000 respectively) (Ministry Of Healthcare, 2020). The app conducts live or near-live tracking of users' locations. The location data and additional diagnostic information from the Bluetooth bracelet is frequently uploaded to the central server through GPS coordinates. Amnesty International assessed the BeAware app as "among the most alarming mass surveillance tools" (Amnesty International, 2020). Additionally, the Ministry of Healthcare of Bahrain requires self-isolating individuals to take random selfies showing their face and the bracelet to prove that they are obeying the quarantine rules (Accessnow, 2020).

Ever since Bahrain became one of the first countries to launch a digital Covid-19 "vaccine passport", the BeAware app has managed the digital vaccination program. Individuals can book the vaccine through the app free of charge. Once vaccinated the app will be able to confirm individual's immunity status via a green "COVID-19 Vaccinated" shield. It also provides information on the type of vaccine received (Anon., 2021).

The app's privacy policy is not specific, but rather a generic privacy policy outlining the terms and conditions on how all data is processed by the eGovernment Authority. It explicitly states that this Authority "may be required to disclose personal data in response to legal requests by government authorities, including meeting national security or law enforcement requirements (SMEX, 2021).

The technical components of Bahrain's contact tracing app raise privacy concerns because the law poses risks of data misuse by the government authorities. A vivid example of data breach was connecting the app to the television show called "Are You at Home?" The host of the show called randomly selected numbers generated through the app. The program offered prizes to those who stayed at home during Ramadan (Woollacott, 2020). The numbers were called out live

on air and those who were at home won a prize. Inclusion in the program was mandatory at the start, but after wide criticism from human rights organizations, Bahrain's Information and eGovernment Authority added an option to opt out. According to the Amnesty International report, the authorities have also published sensitive information about suspected Covid-19 cases online, including individuals' health status, age, gender, and travel history, violating their right to privacy (Amnesty International, 2020). Primary concerns around the BeAware app are linked to government's reliance on real-time location data tracking, use of national ID numbers, and the use of a central server to store the data.

Kuwait

Kuwait does not have a specific data protection legislation, which means there is no clear guidance on how personal data can be collected, stored, transferred, and used. However, certain provisions related to privacy are contained in Kuwaiti E-Transactions Law (No. 20, 2014), the Cybercrime Law (No. 63, 2015) and the constitution. Article 39 of the Kuwait constitution states: "Freedom of postal, telegraphic and telephone correspondence is safeguarded, and confidentiality is guaranteed. Messages may not be monitored except in instances specified by law in accordance with those procedures" (DLA Piper, 2021). The E-Transactions Law requires that personal status, health status, financial information and other personal information is stored confidentially. The law stipulates that client consent is required for the disclosure of their data. The Cybercrime Law protects data and information and specifies the penalties and fines between KD 5 thousand and 20 thousand (USD17 thousand and USD65 thousand) and up to three years of imprisonment. However, there is no authority to enforce the law, determine the rights of data subjects and specify the responsibility of data controllers (SMEX, 2021).

COVID-19 App: Shlonik

In April 2020, the Kuwait Ministry of Health launched a mobile app called "Shlonik" to monitor arrivals in Kuwait. Everyone entering the country is obliged to register with their national ID number and wear the bracelet, which is given to them at the airport. The app and the bracelet

are linked and track the movements of individuals. During the first check-in, individuals have to send a voice recording and take a photo of themselves, which clearly shows their face (Arab Times, 2020). The Ministry of Healthcare can contact people in quarantine at random and request live selfies. Individuals breaching their house quarantine may be fined for KD5 thousand (USD15 thousand) and/or be imprisoned for three months (Library of Congress, 2020). Amnesty International issued a report assessing the app as one of the most invasive Covid-19 contact tracing applications, as the app tracks the movements of users in real-time (Amnesty International, 2020). The app does not have a privacy policy – the link goes directly to the Kuwait government online privacy policy.

There is a lack of transparency regarding the app and there is not much information on how the data is collected, stored, and processed. According to the app description, the data is uploaded to the government's centralized server and requires a national ID number and phone number during registration. It is unclear how long the data is stored for and how it is destroyed later. Further, due to the lack of a data protection framework, there is no functional oversight mechanisms to ensure that the available data privacy provisions are enforced in good faith.

IV. Impact on the human rights of vulnerable populations

All around the globe, the Covid-19 pandemic has disproportionately affected socio-economically vulnerable populations. This is especially true in the less developed, emerging economies and states with discriminatory legal frameworks and restrictive social norms (Organisation for Economic Cooperation and Development, 2020). Women, youth, migrant workers, and minorities have been particularly affected. While academic literature describes in detail the consequences of the pandemic on vulnerable population, little research exists on the effects of Covid-19 contact tracing apps on these populations in the MENA region. A number of international organizations, local civil society groups, and journalists have expressed concerns about the raft of emergency powers being deployed by governments in particular through digital technology (Article19, 2020). Covid-19 mobile apps that track movements can enable real-time surveillance, which poses a privacy threat for everyone and especially marginalized groups that

have historically experienced discrimination and disadvantaged treatment (Health and Human Rights Journal, 2020).

The Middle East region has a history of using technology to surveil journalists, activists, and political dissidents. One of the recent most dramatic cases is the death of Saudi journalist Jamal Kashoggi, whom Saudi authorities were tracking using a spyware system. Similarly, many other Middle Eastern countries have used spyware technologies. To name a few: United Arab Emirates has used the "Karma" spyware system to spy on its citizens; Saudi Arabia used the "Pegasus" system; Bahrain spied on the activist Abdul Ghani al-Khanjar, who was tortured while being shown his own intercepted messages (The Tahrir Institute for Middle East Policy, 2019).

Because of its poor human rights record and history of surveillance, deploying contact tracing apps potentially could have longer lasting and detrimental effects on the lives of MENA citizens.

V. Conclusion and Recommendations

The pandemic response in the MENA region has varied. While the oil-rich Gulf States have managed to flatten the curve, the poorer countries lag far behind. All 19 countries instituted a form of strict containment measures, with full to partial lockdowns and nighttime curfews and have deployed various technological and policy tools to halt the spread. Fifteen of the 19 countries developed contact tracing applications and while the possibility of using technology to address a healthcare crisis is a positive phenomenon of this century, it also opens doors to more invasive forms of surveillance. To ensure the protection of human rights governments should consider the following:

- Governments must build and deploy contact tracing technological tools that adhere to human rights standards and protect the privacy of individuals using the app.
- Governments that have already deployed Covid-19 contact tracing applications must make the apps *voluntary* and ensure that their technological features are transparent and accessible for everyone, especially when it comes to sharing, storing and processing health data.

- Governments should use the decentralized system of storing the data. A pandemic is no excuse to collect and store personally sensitive information on the governments' official servers. This leaves the door wide open for mass surveillance, privacy invasion, and misuse of personal information.
- The governments in Bahrain and Kuwait should stop sharing individuals' personal information with private entities, which was the case with the Bahrain's "Are You at Home?" TV program.
- Personal data should be kept for a limited timeframe. Afterwards, the data should be erased and only non-identifiable information stored for further statistical or research purposes.
- Governments must adopt robust data privacy laws to protect people's privacy and other fundamental rights. In countries where data privacy laws are scattered among different legislative frameworks or are non-existent, the governments should engage with civil society actors and human rights organizations to ensure that adequate legal protection and privacy safeguards are in place. Countries that have adopted data privacy laws must safeguard that the laws are enforced adequately and in good faith.
- Governments should create an independent regulatory body to enforce the law. Data Protection Authorities should be adequately equipped to enforce the law with the responsibilities of DPAs clearly defined and aligned with international best practices.

Conclusions

Digital surveillance has increased with the Covid-19 pandemic, and how it is managed has led to a debate about the actual impact of contact tracing in handling the crisis. While the use of technology to manage health emergencies is not new, the way in which individual data has been used and the degree of intrusiveness allowed, particularly through contact tracing applications, is of concern, particularly for human rights and data protection. The Office of the UN High Commissioner for Human Rights has previously warned the international community that emergency powers should not be disguised as health measures to target particular individuals and vulnerable populations, nor should they silence the work of democracy and human rights activists (OHCHR, 2020).

Three trends emerge from the findings of our regional report.

The double-edged effect of technology in the fight against a pandemic

While technology is crucial in the fight against the pandemic, its effects are compromised if data is not controlled. Privacy and data protection can be compromised by the numerous and invasive permissions required by many contact tracing applications. It is quite worrying that non-health data can now be easily accessed by government entities, especially in countries where vulnerable populations and activists could be put at risk by these measures. If left unchecked, the data collected could be used for mass surveillance activities that could curtail individual freedoms and threaten democracy. This is also a concern as some of these contact tracing applications have been developed by private companies in countries where data protection laws are not sufficiently comprehensive or properly enforced. There are risks of data being used for commercial purposes and even of data being sold for individual profiling. In addition, most applications ask for various permissions (location, photos, contacts, Wi-Fi connections, usage statistics, etc.), in some cases without providing details about why. These permissions need to be assessed in terms of their contribution to the control of epidemics.

Whether the system is centralized or decentralized has proven to be important. If centralized, the application allows health officials to access the data of people who an infected person has been in contact with. Citizens must upload their device identification and allow their recent contacts to be traced back to a central server, which means that, although identifications can be anonymized, government entities with access to the server can see their entire contact network. If decentralized, the individual's data and recent contacts are retained only on the device. If the person is infected, the data is anonymized and transmitted to the central server. This solution is more advantageous in terms of privacy and data protection, as it does not allow data to be hacked. However, a positive outcome of the pandemic is the development of a decentralized privacy-preserving proximity tracing protocol (Cannataci, 2020). This is a protocol developed by engineers for Bluetooth-based tracking to store the data in the device in such a way that government entities do not know who has been exposed to Covid-19.

COVID-19 health measures as opportunities for human rights violations

Restrictions on movement through lockdowns, curfews, and travel bans have provided opportunities for human rights abuses and violations by some states. In all regions, activists have reported being harassed by law enforcement, both at home and online. State-centric securitization has reduced freedom of expression. This phenomenon has already been highlighted in the crisis literature, which demonstrates that restrictions transformed into long-term laws and policies erode democratic institutions and reduce civic space. To limit the impact of the pandemic, governments need to be pressured to dismantle emergency laws and remove these applications while strengthening their collaboration with civil society organizations that promote democracy and human rights.

A challenge: the lack of comprehensive data protection laws and enforcement authority

Although the lack of comprehensive data protection laws and enforcement authorities varies by region, where data is being used and collected on a large scale during the Covid-19 pandemic, it may go unchecked due to a legislative vacuum. The lack of data protection laws raises concerns about transparency and accountability, particularly in relation to how data is used, stored, and shared, but also in relation to legal recourse. If citizens discover that their data have been misused, they are often left without any legislative support or recourse. Furthermore, there seems to be a lack of space for public debate and participation around the implementation and evaluation of Covid-19 applications. There is an accountability gap that is not sufficiently addressed, either by privacy legislation or by civil society organizations.

In conclusion, the Covid-19 pandemic has shown how governments' response to crises may have negative impacts on human rights and democracy, in line with crisis theory and previous literature. The costs of emergency laws and contact tracing apps on individual freedoms and privacy, human rights and data protection may mean that abuses due to the expansion of state powers will continue until these measures are discontinued. To limit interference with human rights, governments around the world should consider proportionality principles when adopting emergency protocols and conduct thorough evaluations when implementing contact tracing apps as public health measures. This should be done within the framework of data protection legislation and in collaboration with civil society organizations involved in the protection of human rights.

Policy recommendations for the use of contact tracing apps

Accountability.

- Apps should operate within the framework of data protection and privacy laws and involve DPAs in monitoring. Specialized governance frameworks for contact tracing apps need to be created.
- Involve CSOs in design, implementation and evaluation of apps. Create spaces for public discussion.
- Adopt and comply with international standards of monitoring and evaluation, such as the Universal Periodic Review (UPR).

Transparency

- Apps 'functionality, purpose, timeframe, storage, and location of data must be explicitly stated, and consent standards must be met.
- The degrees and conditions of access to data by public and private entities require further clarification in most apps 'privacy policies.

Proportionality

- Allowance for permissions needs to be justified in accordance with their contribution to outbreak control, considering human rights costs.
- Apps should collect the minimum amount of data required for outbreak containment. Data should be anonymized.
- Conduct proportionality evaluations with a public health perspective; avoid considering technological solutions in isolation.

Human Rights

- Adopt a human rights perspective in app design. Conduct evaluations of impact on fundamental rights, particularly in the context of emergency protocols.
- Prevent apps from becoming securitizing tools by limiting their purpose to public health goals. Evaluate the impact on populations with increased risk of social control, such as activists or migrants.
- Apps should be the most accessible possible in order to avoid the exclusion of marginalized groups. Consider the limitations posed by access to technology and internet coverage in developing countries.

References

Literature Review and Conclusions

Amnesty International UK. (2020). *Joint civil society statement: States use of digital surveillance technologies to fight pandemic must respect human rights* [Press Release) 2 April. Available at: https://www.amnesty.org/download/Documents/POL3020812020ENGLISH.pdf

Bengio et al. (2020). The need for privacy with public digital contact tracing during the COVID-19 pandemic, *Lancet Digital Health,* 2(7), pp. 342-344.

Cannataci, J. A. (2020). Report of the Special Rapporteur on the right to privacy. Human Rights Council.

Council of Europe. (2020). *2020 Data Protection Report* Available at: https://rm.coe.int/report-dp-2020-en/16809fe49c (Accessed March 14, 2021)

Gasser et al. (2020). Digital tools against COVID-19: taxonomy, ethical challenges, and navigation aid, *Lancet Digital Health*, 2, pp. 425-434.

Hoffman, A. (2020). The Securitization of the Coronavirus Crisis in the Middle East. *The COVID-19 Pandemic in the Middle East and North Africa,* pp. 10-13.

ITU. (2018). *Achieving universal and affordable Internet in the least developed countries*. International Telecommunications Union. Available at: http://unohrlls.org/custom-content/uploads/2018/01/D-LDC-ICTLDC-2018-PDF-E.pdf

Kandel, N. et al. (2020). Health security capacities in the context of COVID-19 outbreak: an analysis of International Health Regulations annual report data from 182 countries, *The Lancet*, 395(10229), pp. 1047–1053. doi: 10.1016/S0140-6736(20)30553-5

Keeling, M. J., Hollingsworth, T. D. and Read, J. M. (2020). Efficacy of contact tracing for the containment of the 2019 novel coronavirus (COVID-19), *Journal of Epidemiology and Community Health*, 74(10), pp. 861–866. doi: 10.1136/jech-2020-214051

Kretzschmar, M. E. et al. (2020). Impact of delays on effectiveness of contact tracing strategies for COVID-19: a modelling study, *The Lancet Public Health*, 5(8), pp. e452–e459. doi: 10.1016/S2468-2667(20)30157-2

Kucharski, A. J. et al. (2020). Effectiveness of isolation, testing, contact tracing, and physical distancing on reducing transmission of SARS-CoV-2 in different settings: a mathematical modelling study, *The Lancet Infectious Diseases*, 20(10), pp. 1151–1160. doi: 10.1016/S1473-3099(20)30457-6

Lynch, M. (2020). The COVID-19 Pandemic in the Middle East and North Africa. *The COVID-19 Pandemic in the Middle East and North Africa,* pp. 3-6.

Morley, J. et al. (2020). *Ethical guidelines for COVID-19 tracing apps* Available at: https://www.nature.com/articles/d41586-020-01578-0 (Accessed March 14, 2021)

Nunes, J. (2020). The COVID-19 pandemic: securitization, neoliberal crisis, and global vulnerabilization. *Scientific Electronic Library Online.*

OECD. (2020). *Flattening the covid-19 peak: Containment and mitigation policies*. OECD. Available at: http://www.oecd.org/coronavirus/policy-responses/flattening-the-covid-19-peak-containment-and-mitigation-policies-e96a4226/

OHCHR. (2020). COVID-19: States should not abuse emergency measures to suppress human rights UN experts, OHCHR, at: https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=25722&LangID=E

Rolland, A. (2020). *Security Distillery.* (Online) Available at: https://thesecuritydistillery.org/all-articles/the-securitisation-of-covid-19-implications-for-civilian-privacy (Accessed March 14, 2021)

Stritzel, H. (2007). Towards a Theory of Securitization: Copenhagen and Beyond. *European Journal of International Relations,* p. 357–383.

United Nations. (2020). *United Nations Human Rights Office of the High Commissioner.* (Online) Available at: https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=25722&LangID=E (Accessed March 14, 2021)

UN General Assembly. (2020). *Report of the Special Rapporteur on the right to privacy, Joseph A. Cannataci*. Available at: https://undocs.org/A/75/147 (Accessed March 14, 2021)

Zwitter, A. and Gstrein, O.J. (2020). Big data, privacy and COVID-19 – learning from humanitarian expertise in data protection, *Journal of International Humanitarian Aid,* 5(4).

Africa

Access Now. (2020). *Recommendations on privacy and data protection in the fight against COVID-19*. Available at: https://www.accessnow.org/cms/assets/uploads/2020/03/Access-Now-recommendations-on-Covid-and-data-protection-and-privacy.pdf (Accessed March 3, 2021)

Burns, S. (2020). How Anonymized Mobile Data Are Helping Ghana Fight COVID-19, *Global Partnership for Sustainable Development*, May 18. Available at: https://www.data4sdgs.org/news/how-anonymized-mobile-data-are-helping-ghana-fight-covid-19 (Accessed February 20, 2021)

Dadzie, C.E. and Raju, D. (2021). Data-driven social safety net response to the COVID-19 crisis in Ghana, *World Bank Blogs*, January 4. Available at: https://blogs.worldbank.org/nasikiliza/data-driven-social-safety-net-response-covid-19-crisis-ghana (Accessed February 25, 2021)

Dzawu, M.M. (2020). *Covid-19 Contact Tracers in Ghana to Get Help from Mobile Phones*. Available at:https://www.bloomberg.com/news/articles/2020-06-23/vodafone-mtn-can-share-client-data-with-ghana-to-trace-contacts (Accessed March 3, 2021)

European Investment Bank (EIB). (2020). *Africa's digital solutions to tackle COVID-19.* Available at: https://www.eib.org/attachments/country/africa_s_digital_solutions_to_tackle_covid_19_en.pdf (Accessed March 3, 2021)

Ghana Data Protection Commission. (2020). *Privacy Notice*. Available at: https://www.dataprotection.org.gh/privacy-policy (Accessed March 3, 2021)

Ghana Ministry of Communications. (2020). *GH COVID-19* Available at: https://ghcovid19.com/ (Accessed February 25, 2021)

Harrison, P.J. (2021). *Kenya Adopts Trusted Travel Digital Tool for COVID-19 Test Result Verification.* Available at: https://thefintechtimes.com/kenya-adopts-trusted-travel-digital-tool-for-covid-19-test-result-verification/ (Accessed February 20, 2021)

Illori, T. (2020). *Data protection in Africa and the COVID-19 pandemic: Old problems, new challenges and multistakeholder solutions*. Available at: https://www.apc.org/en/pubs/data-protection-africa-and-covid-19-pandemic-old-problems-new-challenges-and-multistakeholder (Accessed February 25, 2021)

International Network of Civil Liberties Organizations (INCLO). (2020). *Kenya: Surveillance tech used to enforce mandatory $65-a-night quarantine.* Available at: https://covid19.inclo.net/2020/07/07/pic-in-kenya-aerial-surveillance-app-mandatory-costly-quarantine/ (Accessed February 25, 2021)

ITU News. (2020). *Ghana launches COVID-19 Tracker App*. Available at: https://www.itu.int/en/myitu/News/2020/05/14/13/43/Ghana-launches-COVID-19-Tracker-App (Accessed February 25, 2021)

Lawyer. (2021). Interview with Kenyan data privacy lawyer. March 2, 2021.

Monyango, F. (2020). *Mask or muzzle: The impact of COVID-19 measures on digital rights in Kenya.* Available at: https://www.apc.org/en/pubs/mask-or-muzzle-impact-covid-19-measures-digital-rights-kenya

Morely, J. et al. (2020). *Ethical guidelines for COVID-19 tracing apps*. Available at: https://www.nature.com/articles/d41586-020-01578-0. (Accessed March 14, 2021)

Mutung'u, G. (2020). Placing all the bets on high technology, in *Data Justice and COVID-19: Global Perspectives*, ed. Linnet, T. et al. (London: Meatspace Press) pp. 178-183.

New African. (2020). *AU, Africa CDC adoption of digital technology set to save lives, revive economies*. Available at: https://newafricanmagazine.com/24738/ (Accessed March 3, 2021)

Nkatha, M. (2020). *Contact-Tracing in Africa Faces Unusual Challenges.* Available at: https://digitalprivacy.news/2020/06/22/qa-kenyan-technology-expert-malcolm-kijirah/ (Accessed February 20, 2021)

Oduro-Marfo, S. (2020). Transient Crisis, Permanent Registries in *Data Justice and COVID-19: Global Perspectives*, ed. Linnet, T. et al., (London: Meatspace Press) pp. 141-144.

Overseas Security Advisory Council. (2021). *Health Alert: Kenya, Kenya Requires Digitally Verified COVID-19 Test To Enter Or Depart*. Available at: https://www.osac.gov/Content/Report/ea5e0ffb-aed5-4bec-a5dd-1a97edb7c823 (Accessed February 25, 2021)

PanaBIOS. (2021). *PanaBIOS.* Available at: https://panabios.org/. (Accessed March 6, 2021)

Parliament of the Republic of Ghana. (2012). *Data Protection Act, 2012.* Available at: http://media.mofo.com/files/PrivacyLibrary/3981/GHANAbill.pdf (Accessed February 27, 2021)

Razzano, G. (2020). *Privacy and the pandemic: An African response*. Available at: https://www.apc.org/en/pubs/privacy-and-pandemic-african-response Accessed February 20, 2021

Republic of Kenya. (2019). *The Data Protection Act*. Available at: http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/2019/TheDataProtectionAct__No24of2019.pdf (Accessed February 25, 2021)

SDSN TReNDs for C4DC. (2020). *Using Mobile Data for Health Monitoring: A Case Study of Data Sharing Between Ghana Statistical Services, Vodafone Ghana, and Flowminder Foundation.* Available at: https://static1.squarespace.com/static/5b4f63e14eddec374f416232/t/5ef206529723f531491dceb0/1592919639048/Ghana+Case+Study_FINAL.pdf (Accessed February 25, 2021)

United Nations Conference on Trade and Development. (2020). *Data Protection and Privacy Legislation Worldwide*. Available at: https://unctad.org/page/data-protection-and-privacy-legislation-worldwide (Accessed March 3, 2021)

World Health Organization (WH0). (2020). *African innovators join the fight against COVID-19.* [Press Release) May 29. Available at: https://reliefweb.int/report/world/african-innovators-join-fight-against-covid-19

Zhang, J., Nonvignon, J, and Mao, W. (2020). How well is Ghana—with one of the best testing capacities in Africa—responding to COVID-19?, *Brookings*, July 28. Available at: https://www.brookings.edu/blog/future-development/2020/07/28/how-well-is-ghana-with-one-of-the-best-testing-capacities-in-africa-responding-to-covid-19/ (Accessed February 20, 2021)

Latin America

Agencia de Acceso a la Información Pública, G. de A. (2020). Tratamiento de datos personales ante el Coronavirus, Gobierno de Argentina. Available at: https://perma.cc/SB6R-DQZ5 (Accessed February 20, 2021)

Ámbito. (2020). Cómo funciona CuidAR, la nueva app de Coronavirus Argentina, Ámbito. Available at: https://perma.cc/FM2A-CNYL (Accessed February 23, 2021)

Amnesty International. (2020). Preocupaciones de derechos humanos de la app Cuidar. Amnesty International Argentina. Available at: https://amnistia.org.ar/los-riesgos-de-la-app-cuidar-algunas-preocupaciones-de-derechos-humanos/

Bojali, P. and Vela-Treviño, C. (2019). Despuntan las reformas en materia de protección de datos en América Latina, Conocimiento abierto. *Interamerican Development Bank*, February 12. Available at: https://blogs.iadb.org/conocimiento-abierto/es/proteccion-de-datos-gdpr-america-latina/ (Accessed January 3, 2021)

Brian-Nougrères, A. (2020). Uruguay -Data Protection Overview, One Trust Data Guidance. Available at: https://www.dataguidance.com/notes/uruguay-data-protection-overview (Accessed February 11, 2021)

Centro de Información Oficial. (2020). Ley No 19869, Normativa y Avisos Legales del Uruguay. Available at: https://www.impo.com.uy/bases/leyes/19869-2020 (Accessed December 12, 2020).

Clarín. (2020). Control social Coronavirus en Argentina: el Gobierno analiza cambios en la app CuidAR, para limitar el monitoreo de la gente, *Clarín Política*. Available at: https://perma.cc/ZK4V-8NU3 (Accessed November 13, 2020)

Venturini, J. (2021). Interview with Regional Coordinator of Derechos Digitales.

El Cronista. (2020). Coronavirus: app para autodetectar síntomas será obligatoria para quienes llegan del exterior. *El Cronista*. Available at: https://perma.cc/5NMW-L4YF (Accessed January 15, 2021)

Fratti, S. (2019). Estudio Centroamericano de Protección de Datos Guatemala. Instituto Panameño de Derecho y Nuevas Tecnologías. Available at: https://www.ipandetec.org/wp-content/uploads/2019/01/EDP_Guatemala.pdf

Global Witness. (2020). COVID-19 tracing apps must not interfere with human rights, May 14. Available at: https://www.globalwitness.org/en/campaigns/digital-threats/covid-19-tracing-apps-must-not-interfere-human-rights/ (Accessed December 20, 2020)

Gobierno de Argentina. (2020). Sistema y aplicación Cuidar, Gobierno de Argentina. Available at: https://www.argentina.gob.ar/jefatura/innovacion-publica/acciones-coronavirus/aplicacion-y-tableros-de-gestion/como-funciona (Accessed February 4, 2021)

IDB. (2020.) COVID-19: Coronavirus UY, Inter-American Development Bank. Available at: https://socialdigital.iadb.org/en/sph/covid-19/digital-solutions/6303 (Accessed December 20, 2020)

In-telligent, (2020), Application Privacy Statement, Privacy Statement Version – 05-01-2020. Available at: https://in-telligent.com/application-privacy-policy-2/ (Accessed December 20, 2020)

Kaminer, R. and Pagola, F. (2021), Why Uruguay's "miracle" Covid-19 app failed to deliver, *Rest of World*, February 12. Available at: https://restofworld.org/2021/uruguay-covid-app-failed-to-deliver/ (Accessed March 1, 2021)

La Nación. (2020). Cómo funciona la app CuidAR, de uso obligatorio para quienes vuelven al trabajo durante la cuarentena, *La Nación*. Available at: https://perma.cc/L8LB-9TMQ (Accessed January 5, 2021)

Mendel, T. and UNESCO Office Quito and Regional Bureau for Communication and Information in Latin America and the Caribbean. (2009). El Derecho a la información en América Latina: comparación jurídica.

Méndez, G. (2020). Giammattei anuncia que estará disponible la app "Alerta Guate", *Soy 502*, March 24. Available at: https://www.soy502.com/articulo/gobierno-lanzara-este-martes-app-alerta-guate-covid-19-32419.

Milano, G. (2020a). Digital Border Declaration 2020 in Coronavirus UY App, Genexus UK and Ireland. Available at: https://www.genexus.io/the-evolution-of-erps-for-companies-2/ (Accessed February 11, 2021)

Milano, G. (2020b), Modeling reality, generating software, Coronavirus UY App: Behind the Screens, April 5. Available at: https://genexus.blog/en_US/general-interest/aplicacion-coronavirus-uy-detras-de-la-pantalla/ (Accessed February 11, 2021)

Ministerio de Justicia y Derechos Humanos Presidencia de la Nación. (2000). PROTECCION DE LOS DATOS PERSONALES. Ley 25.326, Información Legislativa. Available at: https://perma.cc/NE2W-72LH (Accessed January 5, 2021)

Nuestro Diario. (2018). Espionaje ilegal del Gobierno: Aquí está la investigación de Nuestro Diario (Parte I), August 6. Available at: https://nomada.gt/pais/la-corrupcion-no-es-normal/espionaje-

ilegal-del-gobierno-aqui-esta-la-investigacion-de-nuestro-diario-parte-i/ (Accessed January 5, 2021)

OAS. (2021). Normative developments per country, Organisation of American States. Available at: http://www.oas.org/es/sla/ddi/proteccion_datos_personales_dn_guatemala.asp (Accessed February 20, 2021)

Scrollini, F. et al. (2020). Uruguay's COVID-19 contact tracing app reveals the growing importance of data governance frameworks, LSE Latin America and Caribbean blog, August. Available at: https://blogs.lse.ac.uk/latamcaribbean/2020/08/26/uruguays-covid-19-contact-tracing-app-reveals-the-growing-importance-of-data-governance-frameworks/ (Accessed December 12, 2020)

The Bureau of National Affairs. (2015). Privacy and Security Law Report. 14 PVLR 730. Available at: https://iapp.org/media/pdf/resource_center/Privacy_Laws_Latin_America.pdf.

Southeast Asia

Asia Centre. (2020). Covid-19 and Democracy in Southeast Asia, Building Resilience, Fighting Authoritarianism. Available at https://asiacentre.org/covid-19_and_democracy_in_southeast_asia/

Baysa-Barredo. J.M. (2020). Problematizing the Securitization of Covid-19 in Southeast Asia: A Necessary Step Towards an Inclusive, Rights-Centred Normal.

Deloitte South East Asia. (2018). Data and privacy protection in ASEAN. What does it mean for businesses in the region? Available at https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/risk/sea-risk-data-privacy-in-asean.pdf

Mendoza. J. (2020). Contact tracing apps raise data privacy concerns: Inquirer contributor, *The Straits Times* (blog) https://www.straitstimes.com/asia/contact-tracing-apps-raise-data-privacy-concerns-inquirer-contributor.

Kim. S. (2020). Vietnam's contact-tracing app: Public health tool or creeping surveillance? https://southeastasiaglobe.com/bluezone-contact-tracing-app/.

Shepherdson. K. (2020). How intrusive are contact-tracing apps in ASEAN? https://www.techinasia.com/intrusive-asean-contacttracing-apps.

Middle East and North Africa

Accessnow, 2020. *Accessnow.* (Online) Available at: https://www.accessnow.org/covid-19-contact-tracing-apps-in-mena-a-privacy-nightmare/ (Accessed March 11, 2021)

Ali, F. H. A., n.d. *Bahrain - Data Protection Overview.* https://www.dataguidance.com/notes/bahrain-data-protection-overview

Amnesty International. (2019). *Amnesty International.* (Online) Available at: https://www.amnesty.org/en/countries/middle-east-and-north-africa/report-middle-east-and-north-africa/ (Accessed March 22, 2021)

Amnesty International. (2020). *Bahrain, Kuwait and Norway contact tracing apps among most dangerous for privacy.* https://www.amnesty.org/en/latest/news/2020/06/bahrain-kuwait-norway-contact-tracing-apps-danger-for-privacy/

Anon. (2021). *Mobihealthnews.* (Online) Available at: https://www.mobihealthnews.com/news/emea/bahrain-first-country-allow-vaccine-appointment-mobile-app (Accessed March11, 2021)

Arab Times. (2020). *Arab Times.* (Online) Available at: https://www.arabtimesonline.com/news/shlonik-how-are-you-app-monitors-home-quarantined-people/ (Accessed March 22, 2021)

Article19 (2020). *Article19.* (Online) Available at: https://www.article19.org/resources/covid-19-emergency-powers-must-be-kept-in-check/ (Accessed March 11, 2021)

Buzan, B., Waever, O. 2003. Regions and powers: the structure of international security (No. 91). Cambridge University Press

DLA Piper. (2021). *DLA Piper.* (Online) Available at: https://www.dlapiperdataprotection.com/index.html?t=law&c=SA#:~:text=sensitive%20personal%20data-,In%20the%20absence%20of%20specific%20data%20protection%20legislation%2C%20there%20is,definition%20of%20sensitive%20personal%20data.&text=There%20is%20no%20na (Accessed March 11, 2021)

DLA Piper, 2021. *DLA Piper.* (Online) Available at: https://www.dlapiperdataprotection.com/index.html?t=law&c=KW#:~:text=Kuwait%20does%20not%20have%20a,Stored (Accessed March 22, 2021)

GSMA (2019). *Data Privacy Frameworks in MENA*. https://www.gsma.com/mena/wp-content/uploads/2019/06/GSMA-Data-Privacy-in-MENA-Full-Report.pdf

Health and Human Rights Journal. (2020). *Health and Human Rights Journal.* (Online) Available at: https://www.hhrjournal.org/2020/04/contact-tracing-apps-extra-risks-for-women-and-marginalized-groups/ (Accessed March 10, 2021)

Human Rights Watch. (2020). *Covid-19 Apps Pose Serious Human Rights Risks.* https://www.hrw.org/news/2020/05/13/covid-19-apps-pose-serious-human-rights-risks

Library of Congress. (2020). *Global Legal Monitor.* (Online) Available at: https://www.loc.gov/law/foreign-news/article/saudi-arabia-oman-kuwait-ministries-of-health-begin-using-mobile-apps-to-combat-covid-19/ (Accessed March 10, 2021)

Ministry Of Healthcare (2020). (Online) Available at: https://healthalert.gov.bh/en/category/beaware-bahrain-app (Accessed March 22, 2021)

Organisation for Economic Cooperation and Development. (2020). *COVID-19 crisis response in MENA countries.* http://www.oecd.org/coronavirus/policy-responses/covid-19-crisis-response-in-mena-countries-4b366396/

PWC. (2021). *PWC.* (Online) Available at: https://www.pwc.com/m1/en/media-centre/articles/oman-latest-developments-data-protection-cybersecurity.html#:~:text=Oman%20does%20not%20currently%20have,a%20fundamental%20right%20beyond%20this. (Accessed March 11, 2021)

SMEX. (2021). *Data Protection and Privacy Laws In MENA: A Case Study Of Covid-19 Contact Tracing Apps.* https://smex.org/data-protection-and-privacy-laws-in-mena-a-case-study-of-covid-19-contact-tracing-apps-rport/.

The Tahrir Institute for Middle East Policy. (2019). *The Tahrir Institute for Middle East Policy.* (Online) Available at: https://timep.org/reports-briefings/timep-brief-use-of-surveillance-technology-in-mena/ (Accessed March11, 2021)

The Tahrir Institute for Middle East Policy. (2020). *The Tahrir Institute for Middle East Policy.* (Online) Available at: https://timep.org/press/press-releases/timep-joins-109-organizations-on-digital-surveillance-privacy-and-covid-19-statement/
(Accessed March 11, 2021)

Woollacott, E. (2020). *Forbes.* (Online) Available at: https://www.forbes.com/sites/emmawoollacott/2020/06/16/coronavirus-tracing-app-shared-data-with-game-show/?sh=59b84f3768e2 (Accessed March 11, 2021)

Appendices

Appendix 1: Africa contact tracing apps table

Appendix 2: Latin America contact tracing apps table

Appendix 3: South-East Asia contact tracing apps table

Appendix 4: Middle East contact tracing apps table

Appendix 1

Contact tracing apps in Africa

Country	COVID App	Name	Developer	Authorizer	Capabilities	Contact Tracing	Mandatory or Not Mandatory?	GPS or Bluetooth?	Permissions (mic, camera, location, sharing with 3rd parties)	Privacy Policy	Centralized or Decentralized	Google/Apple API?	Number of Downloads	Data Protection Laws	Data Protection Law Link	Draft?
Algeria	Yes	Coronavirus Algérie	Algerian Ministry of Startups	Ministry of Health	Information, Self-Diagnosis, Contact Tracing	Yes	Not Mandatory	GPS	**Location** approximate location (network-based) precise location (GPS and network-based) **Phone** read phone status and identity **Photos/Media/Files** read the contents of your USB storage modify or delete the contents of your USB storage **Storage** read the contents of your USB storage modify or delete the contents of your USB storage **Device ID & call information** read phone status and identity **Other** receive data from Internet view network connections full network access run at startup control vibration prevent device from sleeping	https://www.smartsolutions.hosting/wp-content/uploads/2020/03/Privacy-Policy.htm			100000+	Loi n° 18-07 du 10 juin 2018 relative à la protection des personnes physiques dans le traitement des données à caractère personnel. (in French)	https://www.joradp.dz/jo2000/2018/034/FP10.pdf	
Angola	Yes	CISP COVID-19 Angola	Ministry of the Interior	Ministry of the Interior	Education, Government Guidelines, Case map, Self-diagnosis	No	No	GPS	This app has access to: **Location** precise location (GPS and network-based) **Photos / Media / Files** read the contents of your USB storage modify or delete the contents of your USB storage **Storage** read the contents of your USB storage modify or delete the contents of your USB storage **Other** receive data from Internet view network connections full network access prevent device from sleeping	https://www.cisp.gov.ao:10443/politica-de-privacidade/			1000+	Lei No. 22/11 da Protecção de Dados Pessoais de 17 de Junho (in Portuguese)	https://media2.mofo.com/documents/Law_22_11_Data_Privacy_Law.pdf	
Benin	No													Loi n° 2017-20 portant code du numérique en République du Bénin	https://www.afapdp.org/wp-content/uploads/2018/06/Benin-Loi-2017-20-Portant-code-du-numerique-en-Republique-du-Benin.pdf	
Botswana	Yes	BSafe	Brastorne Enterprises	Government of Botswana	Contact tracing via QR code	Yes	No	No	This app has access to: **Phone** read phone status and identity **Photos/Media/Files** read the contents of your USB storage modify or delete the contents of your USB storage **Storage** read the contents of your USB storage modify or delete the contents of your USB storage **Camera** take pictures and videos **Wi-Fi connection information** view Wi-Fi connections **Device ID & call information** read phone status and identity **Other** receive data from Internet view network connections full network access control vibration prevent device from sleeping	https://drive.google.com/file/d/1KXPTpfRI-1Pakl9XILEjmetcYHxRV3JY/view			100,000+	Bill - Data protection Law 2018, maybe passing in 2020.	https://www.bocra.org.bw/sites/default/files/documents/DataProtectionAct.pdf	Yes
Burkina Faso	Yes	DiagnoseMe	Faso Civic		Self-diagnosis, contact doctor, Education	No	Not Mandatory	GPS	This app has access to: **Location** approximate location (network-based) precise location (GPS and network-based) **Photos/Media/Files** read the contents of your USB storage **Storage** read the contents of your USB storage **Camera** take pictures and videos **Microphone** record audio **Other** receive data from Internet view network connections full network access change your audio settings run at startup control vibration prevent device from sleeping	https://diagnoseme.fasocivic.org/		No	100+	Loi n° 010-2004/AN Portant Protection des Données à Caractère Personnel (in French)	http://www.afapdp.org/wp-content/uploads/2012/01/Burkina-Faso-Loi-portant-protection-des-donn%C3%A9es-%C3%A0-caract%C3%A8re-personnel-20042.pdf	
Burundi	No															
Cape Verde	Yes	ComVida	Cape Verde Government (NOSi)	Cape Verde Government	Self-Registration & Diagnosis, Contact Tracing, Complaint System, Education/Government Information	Yes	Not Mandatory	Bluetooth		https://covid19.cv/				Lei n° 133/V/2001 of 22 January 2001 (in Portuguese)	http://www.afapdp.org/wp-content/uploads/2012/01/Cap-vert-Lei-n%C2%B0133-V-2001-do-22-janeiro-20011.pdf	
Cameroon	No															
Central African Republic	No															
Chad	No													Law 007/PR/2015 on the Protection of Personal Data (in French and Arabic)	https://arcep.td/sites/default/files/Loi-N%C2%B007-PR-2015.pdf	
Comoros	No															

Appendix 1

Contact tracing apps in Africa

Country	COVID App	Name	Developer	Authorizer	Capabilities	Contact Tracing	Mandatory or Not Mandatory?	GPS or Bluetooth?	Permissions (mic, camera, location, sharing with 3rd parties)	Privacy Policy	Centralized or Decentralized	Google/Apple API?	Number of Downloads	Data Protection Laws	Data Protection Law Link	Draft?
Congo, Democratic Republic of the	No															
Congo, Republic of the	No													Loi n° 29-2019 du 10 octobre 2019 portant protection des données à caractère personnel	https://www.sgg.cg/JO/2019/congo-jo-2019-45.pdf	
Cote D'Ivoire	No													Loi n° 2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel (in French)	http://media.mofo.com/files/PrivacyLibrary/3979/Cote-d-voire-loi_2013_450.pdf	
Djibouti	No															
Egypt	Yes	Sehet Misr	Ministry of Health	Ministry of Health	Self-Diagnosis, Alerts when in COVID case area, Reporting own or other potential infections	Yes	Not Mandatory	GPS	**Location** approximate location (network-based) precise location (GPS and network-based) **Photos / Media / Files** read the contents of your USB storage **Storage** read the contents of your USB storage **Other** receive data from Internet view network connections full network access run at startup control vibration prevent device from sleeping	http://www.mohp.gov.eg/		No	1,000,000+	Law on the Protection of Personal Data	https://www.dataguidance.com/sites/default/files/egypt_data_protection_law_arabic.pdf	
Equitorial Guinea	No													Law No. 1/2016, Law on Personal Data Protection	https://platform.dataguidance.com/notes/equatorial-guinea-data-protection-overview	
Eritrea	No															
Eswatini	No													Bill Data Protection, 2013		Yes
Ethiopia	Yes	COVID-19 Ethiopia -Health Worker Training Platform	Federal Ministry of Health	Federal Ministry of Health	Education/Training for Health Workers	No	Not Mandatory		This app has access to: **Wi-Fi connection information** view Wi-Fi connections **Storage** modify or delete the contents of your USB storage read the contents of your USB storage **Photos/Media/Files** modify or delete the contents of your USB storage read the contents of your USB storage **Location** precise location (GPS and network-based) approximate location (network-based) Device ID & call information read phone status and identity **Phone** read phone status and identity **Other** full network access modify global animation speed view network connections prevent device from sleeping run at startup access Bluetooth settings pair with Bluetooth devices	https://digital-campus.org/privacy/			10,000+			
Ethiopia	Yes	Debo	Federal Ministry of Health	Federal Ministry of Health	Contact Tracing	Yes	Not Mandatory	GPS	This app has access to: **Location** approximate location (network-based) precise location (GPS and network-based) **Other** view network connections pair with Bluetooth devices access Bluetooth settings full network access run at startup control vibration	http://debo.ewenet.net/			100+			
Gabon	No													Loi n°001/2011 relative à la protection des données à caractère personnel (in French)	http://www.afapdp.org/wp-content/uploads/2012/01/Gabon-Loi-relative-%C3%A0-la-protection-des-donn%C3%A9es-personnelles-du-4-mai-20112.pdf	

Appendix 1

Contact tracing apps in Africa

Country	COVID App	Name	Developer	Authorizer	Capabilities	Contact Tracing	Mandatory or Not Mandatory?	GPS or Bluetooth?	Permissions (mic, camera, location, sharing with 3rd parties)	Privacy Policy	Centralized or Decentralized	Google/Apple API?	Number of Downloads	Data Protection Laws	Data Protection Law Link	Draft?
Gambia	No													Information and Communications Act No. 2 of 2009 (in English) Bill to be enforced in 2020 : Data protection and Privacy Policy	http://www.moici.gov.gm/sites/default/files/2019-09/IC-Info-Comms-Act-2009.pdf http://www.pura.gm/wp-content/uploads/2019/08/Data-Protection-and-Privacy-Draft-Policy-and-Strategy-August-2019.pdf	
Ghana	Yes	GH COVID-19 Tracker App	Ministry of Communication	Ministry of Communication	- Check coronavirus symptoms - Check your risk of infection - Users near you - Self quarantine management - Event management - In-App reporting - Guidance on COVID-19	Yes	Not Mandatory	GPS	**Device & app history** retrieve running apps **Location** approximate location (network-based) precise location (GPS and network-based) access extra location provider commands **Photos/Media/Files** read the contents of your USB storage modify or delete the contents of your USB storage **Storage** read the contents of your USB storage modify or delete the contents of your USB storage **Camera** take pictures and videos **Wi-Fi connection information** view Wi-Fi connections **Other** receive data from Internet view network connections full network access run at startup control vibration prevent device from sleeping read Google service configuration	https://www.dataprotection.org.gh/privacy-policy			5000+	Data Protection Act (Act No. 843) 2012 - DPA (in English)	http://media.mofo.com/files/PrivacyLibrary/3981/GHANABill.pdf	
Guinea	No													Loi L/2016/037/AN relative à la cyber-sécurité et la protection des données à caractère personnel	https://justiceguinee.gov.gn/laws/loi-l-2016-037-an-relative-a-la-cybersecurite-et-la-protection-des-donnees-a-caractere-personnel/	
Guinea-Bissau	No															
Kenya	Yes	mSafari	Dalariders Logistics, iGov Africa, Fablab Winam	Government	Contact Tracing	Yes	Mandatory for those on public service vehicles	No - QR Code Scanning	This app has access to: **Photos/Media/Files** read the contents of your USB storage modify or delete the contents of your USB storage **Storage** read the contents of your USB storage modify or delete the contents of your USB storage **Other** view network connections full network access	NA		No	Downloaded via APK	The Data Protection Act, 2019	http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/2019/TheDataProtectionAct__No24of2019.pdf	
Lesotho	No													Data Protection Act No. 19 2012 (In English)	http://www.nic.ls/lsnic/community/policies/Data_Protection_Act_2011_Lesotho.pdf	
Liberia	Yes	COVID-19 Symptom Tracker (LR)	National Public Health Institute of Liberia	collaboration between the Ministry of Health, National Public Health Institute of Liberia, Ministry of Transport, Liberian Civil Aviation Authority, Liberia Airport Authority, Executive Committee on Coronavirus, and the Healthcare Federation of Liberia with the support of LINGO	Screening & Reporting	No	Not Mandatory		Location Photos	https://covidliberia.com/privacy.html						
Libya	No															
Madagascar	No													Law No. 38/2014 Protection of personal data (in French)	http://www.afapdp.org/wp-content/uploads/2015/01/Madagascar-L-2014-038-du-09-01-15-sur-la-protection-des-donn%C3%A9es-%C3%A0-caract%C3%A8re-personnel.pdf	
Malawi	No													Bill - Data Protection Act		Yes

Appendix 1

Contact tracing apps in Africa

Country	COVID App	Name	Developer	Authorizer	Capabilities	Contact Tracing	Mandatory or Not Mandatory?	GPS or Bluetooth?	Permissions (mic, camera, location, sharing with 3rd parties)	Privacy Policy	Centralized or Decentralized	Google/Apple API?	Number of Downloads	Data Protection Laws	Data Protection Law Link	Draft?
Mali	Yes	SOS CORONAVIRUS	AGETIC Mali (Government)	AGETIC Mali (Government)	Information, Education	No	Not Mandatory		Location Photos	http://54.38.241.35/soscovid/files/PC.pdf				Lois sur la protection des données à caractère personnel - Loi n° 2013-015 du 21 mai 2013 (in French)	http://www.afapdp.org/wp-content/uploads/2012/01/Mali-Loi-sur-la-protection-des-donn%C3%A9es-personnelles-du-21-mai-2013.pdf	
Mauritania	No													Loi 2017-020 sur la protection des données à caractère personnel	https://www.ohchr.org/Documents/Issues/Opinion/ContentRegulation/Mauritania_2.pdf	
Mauritius	Yes	beSafeMoris	Mauritius Telecom	Ministry of Health and Wellness of Mauritius	Information, Education	No	Not Mandatory		**Photos / Media / Files** read the contents of your USB storage **Storage** read the contents of your USB storage **Wi-Fi connection information** view Wi-Fi connections **Other** receive data from Internet view network connections full network access run at startup control vibration prevent device from sleeping	https://besafemoris.mu/privacy-policy/			100,000+	Data Protection Act No. 20/2017 (in English)	https://www.ilo.org/dyn/natlex/docs/ELECTRONIC/108724/134563/F68698020/MUS108724.pdf	
Mauritius	Yes	epione.net Patients	epione.net		Medical Record storage, connecting with doctors, scheduling appointments	No	Not Mandatory		Location Camera Photo Library							
Morocco	Yes	Wiqaytna (وقايتنا "Our prevention")	Government - Ministry of Interior	Government - Ministry of Interior	Contact tracing	Yes	Not Mandatory	GPS and Bluetooth	This app has access to: **Location** precise location (GPS and network-based) **Other** receive data from Internet full network access view network connections control vibration prevent device from sleeping run at startup read Google service configuration access Bluetooth settings pair with Bluetooth devices	No	Decentralized		1,000,000+	Law No. 09-08/2009 on the protection of people toward data protection of a personal nature	https://www.dgssi.gov.ma/sites/default/files/attached_files/loi_09-08protection_donnees_personnelles.pdf	
Mozambique	No															
Namibia	No													Bill - Electronic Transaction Act of 2019	https://laws.parliament.na/cms_documents/electronic-transactions-e6007fa08d.pdf	Yes
Niger	No													Loi n°2017-28 du 03 Mai 2017 relative à la protection des données à caractère personnel, révisé en 2019 (In French)	https://www.afapdp.org/wp-content/uploads/2017/02/Loi-n%c2%b02017-28-du-03-mai-2017.pdf	
Nigeria	Yes	Lancor COVID check	The Lagos Analysis Corporation		Self-diagnosis for work attendance approval	No				http://www.lancorltd.com/				Data Protection Regulation	https://ictpolicyafrica.org/pt/document/vvvjev9pcvs	
Rwanda	No													Bill - Personal Data Protection, 2019		Yes
Sao Tome and Principe	No													Data Protection Law 2016	https://www2.camara.leg.br/saotomeeprincipe/diarios-da-an/x-legislatura/ii-serie/3.a-sessao-legislativa/DAN01-IIS.pdf/view	
Senegal	Yes	Alerte Santé Sénégal	Fehu Digital Lab		Information & Statistics	No	Not Mandatory		This app has access to: **Location** precise location (GPS and network-based) **Photos/Media/Files** read the contents of your USB storage modify or delete the contents of your USB storage **Storage** read the contents of your USB storage modify or delete the contents of your USB storage **Wi-Fi connection information** view Wi-Fi connections **Other** receive data from Internet view network connections full network access run at startup control vibration prevent device from sleeping	https://fehudigital.com/confidentialite.php			5000+	LOI n° 2008-12 du 25 janvier 2008 portant sur la Protection des données à caractère personnel	http://www.centif.sn/Loi_2008_12.pdf	

Appendix 1

Contact tracing apps in Africa

Country	COVID App	Name	Developer	Authorizer	Capabilities	Contact Tracing	Mandatory or Not Mandatory?	GPS or Bluetooth?	Permissions (mic, camera, location, sharing with 3rd parties)	Privacy Policy	Centralized or Decentralized	Google/Apple API?	Number of Downloads	Data Protection Laws	Data Protection Law Link	Draft?
Seychelles	Yes	Health Travel Authorization	Seychelles Government	Seychelles Government	Negative COVID-19 test and health approval to travel to Seychelles	No	Yes, for travel to Seychelles		This app has access to: **Photos/Media/Files** read the contents of your USB storage modify or delete the contents of your USB storage **Storage** read the contents of your USB storage modify or delete the contents of your USB storage **Camera** take pictures and videos **Other** view network connections full network access run at startup control vibration prevent device from sleeping read Google service configuration	https://seychelles.govtas.com/pages/PRIVACY		No	1000+	Bill - The Data Protection No. 9 of 2003	http://greybook.seylii.org/se/2003-9	Yes
Seychelles	Yes	Lasante Seychelles	Panafricare		Screening and Information	No	No	GPS	**Location** approximate location (network-based) precise location (GPS and network-based) **Other** receive data from Internet view network connections full network access run at startup control vibration prevent device from sleeping	https://lasante.app/privacy.html			1000+			
Sierra Leone	No															
Somalia	No															
South Africa	Yes	COVID Alert South Africa	Department of Health South Africa	Department of Health South Africa	Contact tracing, exposure notifications	Yes	No	Bluetooth	**Wi-Fi connection information** view Wi-Fi connections **Other** view network connections pair with Bluetooth devices full network access run at startup prevent device from sleeping	https://sacoronavirus.co.za/covidalert/privacy-policy		Yes	1,000,000+	Protection of Personal Information Act 4 of 2013	http://www.justice.gov.za/inforeg/docs.html	
South Sudan	No															
Sudan	No															
Tanzania	Yes	CoronaCheck	Aga Khan University		Self-diagnosis, education	No	Not Mandatory		This app has access to: **Other** full network access	https://hospitals.aku.edu/pakistan/Pages/MobileAppPrivacyPolicy.aspx		No	50,000+	Data Protection Bill 2013		Yes
Togo	Yes	TOGO SAFE	Ministry of Posts, Digital Economy and Technological Innovation of Togo	National COVID-19 Crisis Management Committee and the Ministry of Health	Contact Tracing, Self-diagnosis, Quarantine Enforcement, Education	Yes	Mandatory for Travelers arriving in Togo, Voluntary for others	GPS	This app has access to: **Location** approximate location (network-based) precise location (GPS and network-based) **Camera** take pictures and videos **Wi-Fi connection information** view Wi-Fi connections **Other** receive data from Internet view network connections pair with Bluetooth devices access Bluetooth settings full network access run at startup prevent device from sleeping	https://togosafe.gouv.tg/en/privacy-policy/			10,000+	Loi No. 14/2019 relativbe a la protection des donnees a caractere personnelle (In French)	https://jo.gouv.tg/sites/default/files/JO/JOS_29_10_2019-64E%20ANNEE-N%C2%B026%20TER.pdf#page=1	
Tunisia	Yes	E7mi	Private startup	National Observatory for New and Emerging Diseases	Contact Tracing	Yes	Not Mandatory	GPS	This app has access to: **Location** precise location (GPS and network-based) **Other** receive data from Internet pair with Bluetooth devices access Bluetooth settings full network access run at startup	https://www.e7mi.tn/privacy.html	Decentralized	No	50,000+	Loi organique No. 63/2004 portant sur la protection des données à caractère personnelles Organic Act No. 63/2004 on the protection of personal data	http://www.ins.tn/sites/default/files/Loi%2063-2004%20Fr.pdf https://media2.mofo.com/documents/The+Organic+Act+2004-63.pdf	
Uganda	Yes	MOH Uganda Capacity Building App	Ministry of Health	Ministry of Health	Education - Health Worker training	No	Not Mandatory	GPS	This app has access to: **Location** approximate location (network-based) precise location (GPS and network-based) **Phone** read phone status and identity **Photos/Media/Files** read the contents of your USB storage modify or delete the contents of your USB storage **Storage** read the contents of your USB storage modify or delete the contents of your USB storage Wi-Fi connection information view Wi-Fi connections Device ID & call information read phone status and identity **Other** view network connections pair with Bluetooth devices access Bluetooth settings full network access run at startup modify global animation speed prevent device from sleeping	https://digital-campus.org/privacy/		No	1000+	The Data Protection and Privacy Bill, 2015 (in English)	https://ulii.org/system/files/legislation/act/2019/1/THE%20DATA%20PROTECTION%20AND%20PRIVACY%20BILL%20-%20ASSENTED.pdf	Yes
Zambia	No													Data Protection Act, 2020,	http://www.parliament.gov.zm/sites/default/files/documents/related_documents/The%20Data%20Protection%20Bill%2C%202020.pdf	

Appendix 1

Contact tracing apps in Africa

Country	COVID App	Name	Developer	Authorizer	Capabilities	Contact Tracing	Mandatory or Not Mandatory?	GPS or Bluetooth?	Permissions (mic, camera, location, sharing with 3rd parties)	Privacy Policy	Centralized or Decentralized	Google/Apple API?	Number of Downloads	Data Protection Laws	Data Protection Law Link	Draft?
Zimbabwe	No													Bill - Data Protection 2016 (In English)	http://www.techzim.co.zw/wp-content/uploads/2016/08/Zimbabwes-Draft-Data-Protection-Bill-v-1-June-2013.pdf	Yes

Appendix 2

Contact tracing apps in Latin America

Country	COVID App	Developer	Authorizer	Capabilities	Contact Tracing	Mandatory or Not Mandatory?	GPS or Bluetooth?	Permissions	Centralized or Decentralized	Google/Apple API?	Number of Downloads	Data Protection Laws	Data Protection Authority or Enforcement	Privacy Policy
Belize	Belize Travel Health	Government of Belize	Statistical Institute of Belize	Geo-tracking functionality for all travellers during their stay in Belize to assist public health officials in contact tracing.	Yes	Mandatory for people entering the country	GPS	-	-	-	-	No	No	https://www.covid19.bz/privacy-policy/
Costa Rica	EDUS COVID-19	Costa Rican Social Security Fund	-	Manage of medical appointments, self-diagnosis, synchronisation with Google Fit application on your phone, with which the data registered in Google Fit app.	-	Not mandatory	-	Identity find accounts on the device Calendar read calendar events plus confidential information add or modify calendar events and send email to guests without owners' knowledge Contacts find accounts on the device Phone directly call phone numbers Photos/Media/Files read the contents of your USB storage modify or delete the contents of your USB storage Storage read the contents of your USB storage modify or delete the contents of your USB storage Camera take pictures and videos Other receive data from Internet view network connections full network access run at startup control vibration prevent device from sleeping	-	-	1,000,000+	Law n.o 8968	Agency for Data Protection of Inhabitants (Prodhab)	-
El Salvador	No	-	-	-	-	-	-	-	-	-		-	-	
Guatemala	Alerta Guate (discontinued)	In-telligent	Government of Guatemala	risk alert, information,geolocation	Yes	Not mandatory	GPS	location	-	-	100,000+	-	-	-
Honduras	No	-	-	-	-	-	-	-	-	-	-	-	-	-
Mexico	COVID-19 MX	Secretariat of Health	Secretariat of Health	Direct access to the epidemiological health care telephone number. Self-diagnosis. Calls with the emergency systems if necessary. Gather real aggregated data to be able to make better decisions. Locations: Identify the Service Centers closest to your location, you can check by States or through a map that shows you the address and route to get there. Information Tips: It presents you with prevention measures that will help you avoid this and other diseases. News: Access to official information including press conferences and statements from the Ministry of Health. De-escalation: information about the phase in which the states are.	-	Not mandatory	GPS, Blootooth	Location approximate location (network-based) precise location (GPS and network-based) Contacts read your contacts Photos/Media/Files read the contents of your USB storage modify or delete the contents of your USB storage Storage read the contents of your USB storage modify or delete the contents of your USB storage Camera take pictures and videos Other receive data from Internet pair with Bluetooth devices view network connections prevent device from sleeping run at startup access Bluetooth settings control vibration full network access	-	yes	500,000+	Federal Law of Personal Data Protection	Federal Institute of Access to Information	-
Nicaragua	No	-	-	-	-	-	-	-	-	-	-	Law on Personal Data Protection No. 787		
Panama	Protégete Panamá	Ministry of Health	Government Innovation Authority	Contact tracing, exposure notifications	Yes	Not Mandatory	Blootooth	Otro motivo view network connections pair with Bluetooth devices full network access run at startup prevent device from sleeping	-	yes	50.000+	-	National Authority of Transparency and Access to Information	https://storage.googleapis.com/panama-enx/privacy-policy.html

Appendix 2

Contact tracing apps in Latin America

Country	COVID App	Developer	Authorizer	Capabilities	Contact Tracing	Mandatory or Not Mandatory?	GPS or Bluetooth?	Permissions	Centralized or Decentralized	Google/Apple API?	Number of Downloads	Data Protection Laws	Data Protection Authority or Enforcement	Privacy Policy
Argentina	CuidAR	Public Innovation Secretariat, the Ministry of Science and Technology, Sadosky Foundation, the National Council of Scientific and Technical Research and the Chamber of Software Industry	Government	Information, self-diagnose, circulation permit	-	Mandatory for people entering country and people returning to work	GPS	Camera take pictures and videos Location approximate location (network-based) precise location (GPS and network-based) Other receive data from Internet view network connections full network access prevent device from sleeping	centralized	-	10,000,000+	Personal Data Protection Law 253226	Agency for Access to Public Information	https://www.argentina.gob.ar/sites/default/files/terminos_y_condiciones_aplicacion_cuidar_-_covid_19_-_v5.pdf
Bolivia	Bolivia Segura	Agetic Bolivia	Government	Communication with medical staff, information	-	Not mandatory	GPS	Device ID & call information read phone status and identity Phone read phone status and identity Location precise location (GPS and network-based) approximate location (network-based) Other view network connections full network access	-	-	50,000+	-	-	https://boliviasegura.gob.bo/PrivacyPolicy.html
Brazil	Coronavirus-SUS	Government of Brazil	Ministry of Health	Communication with medical staff, information	yes	Not mandatory	Blootooth	Other receive data from Internet view network connections pair with Bluetooth devices full network access run at startup control vibration prevent device from sleeping	-	yes	5,000,000+	General Law for Data Protection	National Data Protection Authority	https://validacovid.saude.gov.br/politica-privacidade
Chile	CoronApp	Digital Government	Government	Information, self-diagnosis	-	Not mandatory	GPS	Multimedia, location,	-	-	100,000+	Law 19.628	-	yes
Colombia	Coronapp	National Health Institute	Government	Self-diagnosis and those of family members. Receive recommendations according to the state of health after making the self-diagnosis. Obtain mobility status Information Data is geo-referenced.	yes	Not mandatory	GPS, Blootooth	Phone directly call phone numbers read phone status and identity Contacts read your contacts Device ID & call information read phone status and identity Location approximate location (network-based) precise location (GPS and network-based) Other receive data from Internet access Bluetooth settings prevent device from sleeping pair with Bluetooth devices set an alarm full network access view network connections run at startup	-	-	10.000.000+	Law 1581 of 2012	Delegation for Data Protection	https://www.ins.gov.co/Normatividad/PoliticasInstitucionales/politica-de-tratamiento-de-informacion-coronapp-colombia.pdf
Ecuador	CovidEC	Ministry of Telecommunications	Government	Self-diagnosis, news, information	-	Not mandatory	GPS	Location approximate location (network-based) precise location (GPS and network-based) Other view network connections full network access	-	yes	10,000+	-	-	-
French Guinea	No	-	-	-	-	-	-	-	-	-	-	-	-	-
Guayana	No	-	-	-	-	-	-	-	-	-	-	-	-	-

Appendix 2

Contact tracing apps in Latin America

Country	COVID App	Developer	Authorizer	Capabilities	Contact Tracing	Mandatory or Not Mandatory?	GPS or Bluetooth?	Permissions	Centralized or Decentralized	Google/Apple API?	Number of Downloads	Data Protection Laws	Data Protection Authority or Enforcement	Privacy Policy
Paraguay	COVID-19 PY	Government	Government	Self-diagnosis, location, notify physical contact, information.	yes	Not mandatory	GPS	Device & app history retrieve running apps Location approximate location (network-based) precise location (GPS and network-based) access extra location provider commands Photos/Media/Files read the contents of your USB storage modify or delete the contents of your USB storage Storage read the contents of your USB storage modify or delete the contents of your USB storage Other control location update notifications receive data from Internet view network connections full network access run at startup prevent device from sleeping	-	-	5.000+	no	no	https://www.mspbs.gov.py/covid-19.php
Peru	Peru en tus manos	SUNAT	Government	Self-diagnosis, information on risk zones, news, location.	-	Not mandatory	GPS	Location	-	-	-	Law 29733	National Authority of Data Protection	-
Suriname	No	-	-	-	-	-	-	-	-	-	-	-	-	-
Uruguay	CoronavirusUY	ThalesLab, Genexus and AGESIC.	Ministry of Health	Information, medical attention (e-health), contact tracing and alerts of exposure.	yes	Not mandatory	Blootooth	Microphone record audio Camera take pictures and videos Other receive data from Internet prevent device from sleeping change network connectivity pair with Bluetooth devices full network access view network connections run at startup control vibration	decentralized	-	500,000+	Protection of Personal Data Law Nº 18331	Uruguayan Data Protection Authority	https://www.gub.uy/ministerio-salud-publica/comunicacion/publicaciones/politica-privacidad-app-coronavirusuy
Venezuela	No	-	-	-	-	-	-	-	-	-	-	-	-	-
Cuba	No	-	-	-	-	-	-	-	-	-	-	-	-	-
Dominican Republic	COVID-RD	República Digital	Government	Self-diagnosis, contact tracing, information, chatbot, news.	yes	Not mandatory	GPS, Blootooth	Device & app history retrieve running apps Location approximate location (network-based) precise location (GPS and network-based) access extra location provider commands Photos/Media/Files read the contents of your USB storage modify or delete the contents of your USB storage Storage read the contents of your USB storage modify or delete the contents of your USB storage Wi-Fi connection information view Wi-Fi connections Other receive data from Internet view network connections create accounts and set passwords pair with Bluetooth devices access Bluetooth settings change system display settings disable your screen lock full network access read sync settings run at startup control vibration prevent device from sleeping toggle sync on and off Google Play license check	-	-	10,000+	Law 172-13	-	https://docs.google.com/document/d/1fVXZ411uMP-b88GcaaeZG9cEMjje4INJY2-Q71XEyfQ/edit
Haiti	No	-	-	-	-	-	-	-	-	-	-	-	-	-

Appendix 3

Contact tracing apps in South East Asia

Country	COVID App	Developer	Authorizer	Capabilities	Contact Tracing	Mandatory or Not Mandatory?	GPS or Bluetooth?	Permissions	Developer's privacy policy	Centralized or Decentralized	Google/Apple API	Number of Downloads	Data Protection Laws	Data Protection Authority or Enforcement
Brunei	BruHealth	E-Government National Center + Ministry of Health of the Government	E-Government National Center + Ministry of Health of the Government	1. Real time dashboard for Brunei and global COVID-19 situation 2. Density map of activity traces of confirmed patient 3. Map of medical resources 4. COVID-19 self-screening tool 5. Health Clearance Form to get a personal assessment code to participate in activities. 6. Press releases and health education information 7. Bluetooth and GPS tracking for close contact tracing.	Yes	Mandatory for entering all business premises	GPS and network-based + Bluetooth	Photos/Media/Files/Storage - modify or delete the contents of your USB storage - read the contents of your USB storage Microphone - record audio Wi-Fi connection information - view Wi-Fi connections Calendar - add or modify calendar events and send email to guests without owners' knowledge - read calendar events plus confidential information Camera - take pictures and videos Phone - read phone status and identity - directly call phone numbers Device ID & call information - read phone status and identity Location - approximate location (network-based) - precise location (GPS and network-based) - access extra location provider commands Other - receive data from Internet - access Bluetooth settings - control flashlight - run at startup - prevent device from sleeping - pair with Bluetooth devices - view network connections - control vibration - change your audio settings - full network access	Yes https://www.healthapp.gov.bn/covid19/bruhealth/privacy_policy.html	Centralized		100,000+ (Google Play)	no comprehensive law on data protection, but Data Protection Policy	No
Cambodia	Not really (Healthy Home Self-Quarantine App)													
East Timor	NO													
Indonesia	Peduli Lindungi	designed by the Ministry of Communication and Information Technology (Kominfo) and the Ministry of SOEs	supported by the Ministry of Communication and Information, the Ministry of Health, the Ministry of SOEs and the National Disaster Management Agency.	relies on community participation to share location data with each other while traveling to trace the contact history of sufferers of COVID-19, uses bluetooth to record the information needed, dta exchange when there are other gadgets within the Bluetooth radius that are also registered, identify people who have been in close proximity to people who tested positive for COVID-19, contacted by a health worker if you have been within a certain distance with a positive COVID-1 sufferer	Yes	No	GPS and network-based + Bluetooth	Camera - take pictures and videos Wi-Fi connection information: view Location - approximate location (network-based) - precise location (GPS and network-based) Photos/Media/Files/Storage - modify or delete the contents of your USB storage - read the contents of your USB storage Other - receive data from Internet - access Bluetooth settings - pair with Bluetooth devices - view network connections - run at startup - full network access - prevent device from sleeping	Yes but not in english https://pedulilindungi.id/kebijakan-privasi-data The following data may be collected and linked to your identity: - Health & Fitness - Location - User Content - Search History - Browsing History - Identifiers	Centralized		1 000 000+	2016 Electronic Information Law	No
Laos	LaoKYC	SB Lab 856 Co., Ltd	work with the Ministry of Post and Telecommunications	follow official news, digitize contact and profile, location-based outbreak monitoring to provide up to date risk areas, achieved via Simcard registration	Yes	No	GPS and network-based	Location - approximate location (network-based) - precise location (GPS and network-based) Photos/Multimedia Contents/Files/Storage - read the contents of your USB storage - modify or delete the contents of your USB storage Camera - take pictures and videos Others - receive data from Internet - view network connections - full network access - prevent device from sleeping	YES https://sbg.la/about-us/privacy-policy/	Centralized		100 000+ (Google Play)	no statute, but Law on Protection of Electronic Data (2017) and the Law on Prevention and Combating Cyber Crime (2015)	
Malaysia	MySejahtera	Government of Malaysia for the Ministry of Health		Assist the Government in managing and mitigating the COVID-19 outbreak; Help users in monitoring their health throughout the COVID-19 outbreak; Assist users in getting treatment if they are infected with COVID-19; and Locate nearest hospitals and clinics for COVID-19 screening and treatment, allows users to perform health self-assessment on themselves and their family members and monitor their health progress throughout the COVID-19 outbreak, enables the Ministry of Health (MOH) to monitor users' health condition and take immediate actions in providing the	No	No	GPS and network-based	Location - approximate location (network-based) - precise location (GPS and network-based) Mobile - directly call phone numbers Photos/Multimedia Contents/Files/Storage - read the contents of your USB storage - modify or delete the contents of your USB storage Camera - take pictures and videos Others - manage document storage - receive data from Internet - view network connections - control flashlight - full network access - prevent device from sleeping	Yes https://mysejahtera.malaysia.gov.my/privasi_en/ The following data may be collected and linked to your identity: Health & Fitness Location Contact Info User Content Identifiers Sensitive Info	Centralized		10 000 000+ (Google Play)	Personal Data Protection Act (PDPA) 2013	Yes, Department of Personal Data Protection
	MyTrace	International Islamic University Malaysia assisted by MIMOS, MaGIC and Google Malaysia	Governemnt of Malaysia and Ministry of Science, Technology and Innovation	community-driven approach where participating devices exchange proximity information whenever an app detects another nearby device with MyTrace installed, enables identification of people who have been in close proximity to an infected person	Yes	No	Bluetooth, GPS and network-based	Device & app history - retrieve running apps Location - approximate location (network-based) - precise location (GPS and network-based) Photos/Media/Files/Storage - read the contents of your USB storage - modify or delete the contents of your USB storage Other - receive data from Internet - view network connections - pair with Bluetooth devices - access Bluetooth settings - full network access - run at startup - prevent device from sleeping	Yes https://www.mosti.gov.my/web/en/privacy/	Centralized		100,000+ (Google Play)	"	"

Appendix 3

Contact tracing apps in South East Asia

	Gerak Malaysia		Malaysian Communications and Multimedia Commission (MCMC) and Royal Malaysia Police	APP DISCONTINUED beta app for contact tracing, latest information from relevant authorities as well as general COVID-19 preventive measures and advice	Yes	No	Bluetooth, GPS and network-based	Photos/Media/Files/Storage - modify or delete the contents of your USB storage - read the contents of your USB storage View Wi-Fi connection information Camera - take pictures and videos Phone - read phone status and identity - Device ID & call information Location - approximate location (network-based) - precise location (GPS and network-based) Other - update component usage statistics - receive data from Internet - pair with Bluetooth devices - view network connections - draw over other apps - read Google service configuration - full network access - prevent device from sleeping	not available		1,000,000+ (Google Play)	"	"
Myanmar	Saw Saw Shar	Myanmar Computer Federation (MCF) for the Coronavirus Disease 2019 (COVID-19) Control and Emergency Response ICT Team	Ministry of Transport and Communication (MOTC) and the Ministry of Health and Sports (MOHS), the Government of Myanmar	1. Health Report: User can record and report his or her health condition related to the symptoms of COVID-19. 2. Notifications and Warnings: Importance notification and warning messages based on locations and possible contacts, lockdown and high-risk areas. 3. Surveillance Dashboard: COVID-19 Dashboard and statistics provided by the Ministry of Health and Sports (MOHS), the Government of Myanmar. 4. Map Assistance: Map of the user current locations and fever clinics and quarantined centers. 5. Emergency Contacts: Official COVID-19 hotlines by regions and states.	Yes	No	Bluetooth, GPS and network-based	Camera - take pictures and videos Photos/Media/Files/Storage - modify or delete the contents of your USB storage - read the contents of your USB storage Device ID and caller information - read phone status and identity Location - precise location (GPS and network-based) Mobile - read phone status and identity Other - receive data from Internet - access Bluetooth settings - control flashlight - prevent device from sleeping - pair with Bluetooth devices - view network connections - control vibration - full network access	Yes https://info.sawsawshar.gov.mm/infosawsawshar/#/privacy policy		100 000+ (Google Play)	Protecting the Privacy and Security of Citizens (Union Parliament Law 5/2017)	No
Philippines	StaySafe PH	Multisys Technologies Corporation	Philippine government, Department of Health (DOH)	health condition reporting, social distancing, and contact tracing system	Yes	No	**Not mentionned?**	Photos/Media/Files/Storage - read the contents of your USB storage - modify or delete the contents of your USB storage Camera - take pictures and videos Other - receive data from Internet - view network connections - full network access - run at startup - control vibration - prevent device from sleeping	Yes https://www.staysafe.ph/data-privacy	Centralized	500 000+ (Google Play)	2012 Data Privacy Act	No
Singapore	Trace Together	Government Technology Agency		notifies you quickly if you've been exposed to COVID-19 through close contact with other TraceTogether users,	Yes	No	Bluetooth, GPS and network-based	Location - approximate location (network-based) - precise location (GPS and network-based) Photos/Media/Files/Storage - modify or delete the contents of your USB storage - read the contents of your USB storage Camera: take pictures and videos Autre - receive data from Internet - access Bluetooth settings - run at startup - prevent device from sleeping - pair with Bluetooth devices - view network connections - control vibration - full network access	Yes https://www.tracetogether.gov.sg/common/privacystatement/index.html **Data Linked to You** Product Personalisation, Contact Info, Name, App Functionality, Contact Info, Phone Number, User Content, Other User Content; Identifiers, User ID **Data Not Linked to You** Analytics, Usage Data, Product Interaction, Diagnostics, Crash Data, Other Diagnostic Data	Decentralized	4.2 million users (source: app website) and 1 million on Google Play	Personal Data Protection Act 2012 (PDPA)	Yes Personal Data Protection Commission ('PDPC')
	SafeEntry				Yes	Yes for entering businesses	Bluetooth, GPS and network-based	Camera - take pictures and videos Photos / Media / Files / Storage - modify or delete the contents of your USB storage - read the contents of your USB storage View Wi-Fi connections Location - approximate location (network-based) - precise location (GPS and network-based) Other - receive data from Internet - view network connections - change network connectivity - pair with Bluetooth devices - read Google service configuration - prevent device from sleeping - access Bluetooth settings - connect and disconnect from Wi-Fi - control vibration - full network access		Centralized	100,000+ (Google Play)		
Thailand	ThaiChana	Krung Thai Bank	Government	check in system to track the movement of people	Yes	No	GPS and network-based	Location - precise location (GPS and network-based) Camera - take pictures and videos Other - receive data from Internet - view network connections - full network access - prevent device from sleeping - read Google service configuration	Redirect to the company's privacy policy https://krungthai.com/en/content/privacy-policy		1,000,000+ (Google Play)		

Appendix 3

Contact tracing apps in South East Asia

	MorChana (+ private apps)	Digital Government Development Agency	Disease Control Department (DCD)	tool to assist Medical Staffs, Government Agencies, Business Owners, and most importantly, YOU in taking care and protect oneself from the spread of COVID-19, collect use and disseminate only necessary data to protect or suppress dangers to life, body, and health of you, the people around you and all citizen, will track infection, probability and risk of COVID-19 and observe the outbreak situation from data provided by you	Yes	No	Bluetooth, GPS and network-based	Device and application history: retrieve running apps Location - approximate location (network-based) - precise location (GPS and network-based) - access extra location provider commands Photos/Media/Files/Storage - read the contents of your USB storage - modify or delete the contents of your USB storage Camera: take pictures and videos Others - receive data from Internet - view network connections - pair with Bluetooth devices - access Bluetooth settings - full network access - run at startup - control vibration - prevent device from sleeping - Google Play license check	Not available **Data Used to Track You** Location: precise Location Contact Info: Physical Address + Phone Number **Data Not Linked to You** Location: Precise Location Contact Info: Physical Address + Phone Number User Content: Photos or Videos	Centralized	5 000 000+ (Google Play)	Thailand's Personal Data Protection Act (PDPA)	Some part post
Vietnam	Bluezone	Bkav	Viet Nam's Ministry of Information and Communications and Ministry of Health	alert if you had close contact with people who have COVID-19	Yes	No	Bluetooth, GPS and network-based	Location - approximate location (network-based) - precise location (GPS and network-based) Photos/Media/Files/Storage - read the contents of your USB storage - modify or delete the contents of your USB storage Camera: take pictures and videos View Wi-Fi connection information Other - receive data from Internet - view network connections - pair with Bluetooth devices - access Bluetooth settings - full network access - run at startup - control vibration - prevent device from sleeping - Google Play license check	Does not use the permission to locate https://bluezone.ai/faq - Data security: Bluezone stores data on your device only, it does not send such data to the system. - No location data collection: Bluezone does not collect data on your location. - Anonymity: All Bluezoners are anonymous to others. Only competent health authorities know those who are infected and those who are suspected of infection due to close contact with COVID-19 cases. - Transparency: The Project is open source under GPL 3.0. license. Users from other countries are free to learn the operations of the system at	Decentralized	10 000 000+ (Google Play)	Law on Information Technology 2006, Law on Cyber Information Security 2019	Yes, Ministry of Information and Communications (MIC)

Appendix 4

Contact tracing apps in Middle East and North Africa

Country	COVID App	Name	Developer	Authorizer	Capabilities	Contact Tracing	Mandatory or Not Mandatory?	GPS or Bluetooth?	Permissions	Developer's Privicy Policy	Number of Downloads	Data Protection	Other	
Algeria	Yes	1. COROVID Rescue 2. Covid app	1.Startup - TECHGRAPH 2.Startup - GOLDEN CORP ALGERIA	Ministry of Health	1. Build a database at the level of the Ministry of Health to identify citizens using a QR Code. 2. Prevention and awareness application that provides users with real-time information on the progress of the virus, spread statistics, but also recommendations and instructions.	1. Yes, using geolocation 2. No	1. No 2. No	1. Both 2. None	Location Approximate location (network-based) Precise location (GPS and network-based) Phone Phone status and identity Photos/Media/Files Contents of USB storage Storage Contents of your USB storage Device ID & call information Other Receive data from Internet View network connections Full network access Run at startup Control vibration Prevent device from sleeping	Yes	Google play - 100 000+	Yes		
Bahrain	Yes	BeAware	e-Government Authority	Government of Bahrain	1. Contact Tracing: Alerts users to get tested once they have been in contact with a positive case. 2. Coronavirus (COVID-19) Test Results: View Coronavirus lab test results once released by the test center. 3. COVID-19 Test Appointment: enables individuals directed by Ministry of Health to book Coronavirus (COVID-19) tests appointments three days prior to self-isolation end date. 4. PCR (COVID-19) Test Certificate: enables travelers from the Kingdom of Bahrain to view and print their (Polymerase Chain Reaction) PCR test certificate that is valid for one month from the last COVID-19 test. 5. Payment for Arrivals Test: enables the individuals entering Bahrain to pay for their Coronavirus (COVID-19) test. 6. Declaration for Exiting Bahrain: enables Bahraini citizens to declare their responsibility for traveling abroad before leaving the country. 7. Announcements: Provides updates from the National Taskforce for Combatting the Coronavirus (COVID-19). 8. Decision Lists: Provides a list of all released decisions regarding the Coronavirus from Kingdom of Bahrain officials. 9. General Guidelines: Provides protective instructions about the Coronavirus such as	Yes	Mandatory	GPS, Bluetooth	Device & app history retrieve running apps Calendar Read calendar events plus confidential information Add or modify calendar events and send email to guests without owners' knowledge Location Approximate location (network-based) Precise location (GPS and network-based) Access extra location provider commands Photos/Media/Files Read the contents of USB storage Modify or delete the contents of your USB storage Storage Read the contents of USB storage Modify or delete the contents of your USB storage Other Receive data from Internet View network connections Pair with Bluetooth devices Access Bluetooth settings Full network access Run at startup Prevent device from sleeping	Yes	Google play - 500 000+	Yes		
Egypt	Yes	Egypt Health	Health and Population Ministry	Health and Population Ministry	1.Sends alerts when a user is approaching an area that contains a large number of coronavirus infections 2. Prevention methods 3. How to boost imune system 4. Communicate with the Ministy of Healthcare	Yes	No	Both	Location Approximate location (network-based) Precise location (GPS and network-based) Photos / Media / Files Read the contents of USB storage Storage Read the contents of USB storage Other Receive data from Internet View network connections Full network access Run at startup Control vibration Prevent device from sleeping	No	Google play - 1 000 000+	Yes		
Iran	Yes	1. AC19 2. Mask	1. Ministry of Health 2. Professors and students from Technology University	1. Ministry of Health 2. Ministry of Health	1. Detect Covid 19 with YES/NO questions 1.2. Detect infected individuals 2. Awareness raising 2.1. Close contact monitoring	1. Yes 2. Yes	1. No 2. No	GPS, Bluetooth				Yes	AC19 and Mask apps were removed from app store	
Iraq	No											No		

Appendix 4

Contact tracing apps in Middle East and North Africa

Country	COVID App	Name	Developer	Authorizer	Capabilities	Contact Tracing	Mandatory or Not Mandatory?	GPS or Bluetooth?	Permissions	Developer's Privicy Policy	Number of Downloads	Data Protection	Other	
Israel	Yes	HaMagen	Ministry of Health	Ministy of Health	1. Crosses the location with the route maps of the verified corona patients and provides updates in case of overlap. Allows to receive alerts on location and time about the exposure to a diagnosed patient 2. Retains information about locations solely on the device for 14 days and cross-references this information with the Ministry of Health's updated epidemiological data. The Ministry of Health app runs in the background and your information remains on your device only.	Yes	No	GPS, Bluetooth	Device & app history Retrieve running apps Location Approximate location (network-based) Precise location (GPS and network-based) Access extra location provider commands Wi-Fi connection information view Wi-Fi connections Other Receive data from Internet View network connections Pair with Bluetooth devices Access Bluetooth settings Full network access Run at startup Draw over other apps Control vibration Prevent device from sleeping Set an alarm	Yes	Google play - 1 000 000+	Yes		
Jordan	Yes	AMAN	Tech volunteers	Ministry of Health	1. Anonymous GPS data to detect exposure to COVID-19 patients. Once downloaded AMAN stores data about their location points for the past 14 days. If someone using AMAN is diagnosed with coronavirus by the Ministry of Health, the people who have been recently in contact with her/him will be notified through the app	Yes	No	Both	This app has access to: Device & app history retrieve running apps Location approximate location (network-based) precise location (GPS and network-based) access extra location provider commands Wi-Fi connection information view Wi-Fi connections Other receive data from Internet view network connections full network access	Yes	Google play - 1 000 000+	No		
Kuwait	Yes	Shlonik	Kuwait Central Agency of Information Technology	Minsitry of Health	1. Latest health updates 2. A health Bot 3. A self check-in mechanism for quarantined patients 4. Vitals reporting and a communication tool with the MOH medical teams	Yes	Yes	GPS, real-time tracking	Wi-Fi connection information view Wi-Fi connections Microphone Record audio Device & app history Retrieve running apps Location Precise location (GPS and network-based) Access extra location provider commands Approximate location (network-based) Storage Modify or delete the contents of USB storage Read the contents of your USB storage Camera Take pictures and videos Phone Directly call phone numbers Read phone status and identity Photos/Media/Files Modify or delete the contents of your USB storage Read the contents of your USB storage Device ID & call information Read phone status and identity Other Receive data from Internet Full network access Change your audio settings View network connections Control vibration	The site does not open	Google play - 100 000+	Yes		
Lebanon	Yes	Ma3an	American University of Beirut, TedMob	Ministry of Health	1. Contact tracing and exposure notification app 2. If the person tests positive for COVID-19, he/she can consent for MoPH to use the information collected of those who were in their proximity to notify people who may have been exposed. 3. Ma3an uses the Bluetooth® technology on the mobile phone to broadcast its presence anonymously to other mobile devices. The system is designed to be energy-efficient, and it does not collect any geolocation or GPS data. 4. When your app detects another device with the Ma3an app, a randomly generated number is exchanged between the devices and stored locally on each device. 5. If a person tests positive for COVID-19, the can consent for MoPH to use the information collected of those who were in their proximity to notify people who may have been exposed. 6. If they have been exposed to the virus by someone they have been in close contact with, the MoPH will be able to contact you quickly so you can get the support you need, lowering the risk of serious consequences.	Yes	Not mandatory	Both	Location Precise location (GPS and network-based) Other Receive data from Internet View network connections Pair with Bluetooth devices Access Bluetooth settings Full network access Run at startup Control vibration Prevent device from sleeping	Yes	Google play - 50 000+	Yes		

Appendix 4

Contact tracing apps in Middle East and North Africa

Country	COVID App	Name	Developer	Authorizer	Capabilities	Contact Tracing	Mandatory or Not Mandatory?	GPS or Bluetooth?	Permissions	Developer's Privicy Policy	Number of Downloads	Data Protection	Other	
Libya	Yes	Speetar	Ministery of Health (MoH) and the National Center for Disease Control (NCDC)	Ministery of Health (MoH) and the National Center for Disease Control (NCDC)	1. Source about the coronavirus disease. It has a screening tool so that a person can find out what he/she should do in case contracted with virus. 2. It gives access to resources one may need to feel supported and informed 3. Links you to specialists at the National Center for Disease Control to evaluate condition and help to schedule a coronavirus test if needed.	Yes	No	Both	Phone Read phone status and identity Location Precise location (GPS and network-based) Approximate location (network-based) Device ID & call information Read phone status and identity Photos/Media/Files Modify or delete the contents of your USB storage Read the contents of your USB storage Contacts Read your contacts Identity Read your own contact card Wi-Fi connection information View Wi-Fi connections Storage Modify or delete the contents of your USB storage Read the contents of your USB storage Other Receive data from Internet Full network access Prevent device from sleeping View network connections Control vibration	No	Google play - 5000 +	No		
Morocco	Yes	WIQAYTNA	Ministry of Health Ministry of Interior	Ministry of Health	1. Helps to notify the user in the event that another user has been near him/her during the last 21 days, and it has been confirmed that he/she is infected with the virus	Yes	No	Bluetooth, GPS	Location Precise location (GPS and network-based) Other Receive data from Internet Full network access View network connections Control vibration Prevent device from sleeping Run at startup Read Google service configuration Access Bluetooth settings Pair with Bluetooth devices	No	Google play - 1 000 000+	Yes		
Oman	Yes	1.Tarrasud 2. Tarrasud +	1. Ministry of Health 2. Oman Information Technology and Communications Group, eMushrif company, and Oman Broadband company	Ministry of Health	1. Track COVID-19 infection rates and monitor infected individuals in quarantine 2. Enhance the Ministry of Health's current monitoring system by diagnosing, following up, and tracking the medical condition of individuals infected with COVID-19, who are under quarantine, by using artificial intelligence technology and advanced tracking technologies.	Yes	Yes	GPS	This app has access to: Location precise location (GPS and network-based) approximate location (network-based) Storage read the contents of your USB storage modify or delete the contents of your USB storage Camera take pictures and videos Photos/Media/Files read the contents of your USB storage modify or delete the contents of your USB storage Other receive data from Internet full network access access Bluetooth settings pair with Bluetooth devices prevent device from sleeping run at startup view network connections control vibration	Yes	Google play - 100 000+	No	hand braselet	

Appendix 4

Contact tracing apps in Middle East and North Africa

Country	COVID App	Name	Developer	Authorizer	Capabilities	Contact Tracing	Mandatory or Not Mandatory?	GPS or Bluetooth?	Permissions	Developer's Privicy Policy	Number of Downloads	Data Protection	Other	
Qatar	Yes	EHTERAZ	Ministry of Health	Ministry of Health	1) Provide alerts or notifications when members of the public are exposed to a suspected, infected, or confined person through prompt, accurate, digital contact tracing. 2) Provide a visual QR code showing infection and/or vaccine status (when available) to other individuals for safe interaction with the wider community. 3) Identify locations with high infection rates in order for the relevant authorities to provide prompt action to prevent further spread and higher risk exposure to members of the public. 4) Provide official announcements on health, social distancing, containment efforts, and up to date COVID-19 statistics.	Yes	Yes, people who don't use the app can face up to three years in jail	GPS and Bluetooth	Location Approximate location (network-based) Precise location (GPS and network-based) Phone Directly call phone numbers Read phone status and identity Photos / Media / Files Read the contents of your USB storage Modify or delete the contents of your USB storage Storage Read the contents of your USB storage Modify or delete the contents of your USB storage Device ID & call information Read phone status and identity Other Receive data from Internet View network connections Pair with Bluetooth devices Access Bluetooth settings Disable your screen lock Full network access Run at startup Draw over other apps Prevent device from sleeping	Yes	Google play - 1 000 000+	Yes		
Saudi Arabia	Yes	Tabaud	National Information Center NIC of the Saudi Data and Artificial Intelligence Authority SDAIA	Ministry of Health	1. Notifying people if they had contact with others confirmed to be infected with coronavirus also 2. Provide them help by sending their health forms to the Ministry of Health to provide them necessary medical support according to the status and progress of the case 3. Enable those confirmed to be infected with coronavirus to voluntarily share their tests' results with people they had contact with during the past 14 days.	Yes		Bluetooth	Other receive data from Internet full network access prevent device from sleeping run at startup view network connections pair with Bluetooth devices	Yes	Google play - 1 000 000+	No. Protection provided under Sharia laws		
Tunisia	Yes	E7mi	Startup	Ministry of Health	1. Digital tracing application, aimed to help reduce the spread of the virus 2. Once the application is downloaded and installed, it automatically begins to detect and store the interactions that have occurred, that is, whenever you are within a radius of a few meters from another person with the 'application, without revealing the identity of the user in the context of respecting personal data.	Yes	No	Both	Rental Precise location (GPS and network-based) Other Receive data from Internet Pair with Bluetooth devices Access Bluetooth settings Full network access Run at startup	Yes	Google play - 50 000+	Yes		
United Arab Emirates	Yes	ALHOSN UAE	Ministry of Health and Prevention, Abu Dhabi Health Authority and Dubai Health Authority	Ministry of Health and Prevention	1. Combines the features of STAY HOME and TRACE COVID 2. The app can also help trace people who may have come within close proximity to confirmed COVID-19 cases for an extended period of time. It uses short-distance Bluetooth signals to determine when your phone is near another phone that also has the app installed. Both phones exchange anonymized IDs which are then stored in encrypted form on your phone. Using the anonymized IDs, health authorities can quickly identify and contact people at risk of infection so they can be retested.	Yes	No	Bluetooth	Location Approximate location (network-based) Precise location (GPS and network-based) Photos / Media / Files Read the contents of your USB storage Modify or delete the contents of your USB storage Storage Read the contents of your USB storage Modify or delete the contents of your USB storage Camera Take pictures and videos Other Receive data from Internet View network connections Pair with Bluetooth devices Access Bluetooth settings Full network access Run at startup Prevent device from sleeping	Yes	Google play - 1 000 000+	No		
Palestine	No											No		
Yemen	No											Yes		