KONRAD ADENAUER STIFTUNG

4th November 2020

With the smartphone against viruses

Constitutional consideration of corona apps in five regions of the world

Pavel Usvatov, Hartmut Rank, Stanislav Splavnic, Gisela Elsner, Aishwarya Natarajan, Marie-Christine Fuchs, Magdalena Schaffler, Malte Gaier, Anja Finke, Arne Wulff

With the help of the corona app, Covid-19 infection pathways should become traceable. Most countries around the world have introduced these apps. We are looking at the regions South-East Europe, Asia, Latin America, the Middle East, North Africa and Sub-Saharan Africa. How is the legal framework on site? What about the practical implementation? What problems have arisen?

Table of Contents

Introduction

Pavel Usvatov

Since 16 June 2020, the "Corona Warning App" developed by SAP and T-Systems (Telekom) on behalf of the German government has been available for download and installation on smartphones in Germany. It is intended to become a "companion and protector" and help to interrupt chains of infection..[1] By means of a Bluetooth connection, smartphones on which the app is installed can recognize each other, and if the user stays at a distance of less than two metres for more than 15 minutes, the data (anonymous ID, time, duration and signal strength) are stored locally on the devices. In case of an infection, the person himself decides whether he wants to warn the contact persons (and only them) via the app; however, this requires confirmation of the infection by a corona test laboratory by means of a QR code or a TAN. By the end of July, the app had already registered over 16 million downloads..[2]

The introduction of the tracing[3] app was accompanied in this country by an ongoing debate on the legality of its use, which was questioned in particular by data protectionists..[4] The developers and the German government emphasize that the data is safely protected against misuse by the decentralized storage approach and the publicly accessible source code of the app. Meanwhile, the IT experts at the Technical University of Darmstadt and the Universities of Marburg and Würzburg were able to prove "that external attackers can create detailed movement profiles of corona infected persons and, if necessary, identify the persons concerned. Contact information could also be manipulated [...]."[5] For its part, the FIfF e.V. points to the weaknesses in the , required by Art. 35 , which must be implemented as a matter of urgency) that still exist despite the great progress that has been made, and maintains its critical stance..[6]

Despite the above-mentioned complaints, however, it can be stated that the criticism is of a very high level: It is not about the fear that the government and government agencies could misuse the data, but rather about how the business community handles the app and the data. Above all, Apple and Google are mentioned, which are able to design the IT interfaces in a one-sided way and thus also gain control over the data (so-called Google-Apple-Protocol, GAP, which is said to be susceptible to creating motion profiles);.[7] there is also concern, for example, that the app could be turned into a kind of "ticket" in the private sector, thereby indirectly undermining the voluntary nature of its use..[8]

The constitutional debate in Germany and the EU has not and is not directly concerned with the tracing apps themselves, which are offered in many places and are usually discussed in connection with the , but with the restrictions on civil liberties and "emergency regulations" in general,.[9] which in southern and south-eastern Europe in particular, but also, for example, in the case of our western neighbour France, went hand in hand with intensive interference in the fundamental rights of the population and were to some extent garnished with war rhetoric that was rather unfamiliar to the younger generation of Europeans..[10]

In the following five sections, the authors deal with the technical and legal framework conditions for the introduction of corona tracking apps in five regions of the world: in South-Eastern Europe, in Asia, in Latin America, in the MENA region (Middle East and North Africa) and in sub-Saharan Africa. The sixth section summarizes developments and legal challenges.

I. South-East Europe

Hartmut Rank, Stanislav Splavnic

At the beginning of the pandemic in spring 2020, many countries in South-East Europe were initially much less affected by it than South, Central or Western European countries such as Italy, Spain, France and the UK. However, despite low infection rates, measures were taken very quickly in the Balkans, and on a larger scale than in Germany, which restricted the civil liberties of citizens. The two main reasons were:

On the one hand, a considerable proportion of the population of all South-East European countries, whether or not they are members of the EU and therefore benefit from the free movement of labor, works in other EU countries. They commute regularly between their home countries and places of work, especially in the summer months, but also on religious holidays in spring. The fear of these states to "import" many infection cases from the hotspot - at that time in northern Italy - therefore seemed real. Among the first known corona infection cases in March were Albanian and Romanian citizens traveling back from Italy.

On the other hand, the health care systems of South-East European countries are overall much less efficient. This is not only a question of financing hospitals (especially in terms of equipment), which actually had much less capacity to treat highly infectious, communicable respiratory diseases when the crisis broke out. It is above all also a question of the shortage of medical staff: the migration of well-trained doctors and nurses, especially to Western Europe over the last three decades, has left noticeable gaps in state hospitals.

The rigid initial restrictions in the region can to a large extent be explained by the authorities' and many citizens' concerns about a rapid overloading of the desolate health care systems. Many governments quickly resorted to severe cuts such as curfews lasting several weeks or months. Some countries introduced the obligation to carry special passes, for example in Romania a certificate signed by the employer for the journey to work. Infringements were criminalized and punishable by heavy fines, which were also used intensively in Romania, among others.

Legal framework

The constitutions of most countries in the region have emergency clauses, which were triggered at different times after the outbreak of the pandemic. The constitutions only allow restrictions to civil rights in line with the principle of proportionality. Furthermore, almost all states in South-East Europe (with the exception of **Kosovo**) are also signatories to the European Convention on Human Rights, whose emergency clause, Art. 15 ECHR[11], also allows the proportionate restriction of the rights and freedoms set out in the Convention. Some States have made use of the ECHR emergency clause in recent months in the context of the corona pandemic. Other countries, which had no infection cases for a long time (e.g. Montenegro) have not yet made use of this possibility.

Although the decision-making process in South-East European countries was also characterized to a certain extent by emergency measures (example **Romania**: adoption of "military (emergency) regulations" by the Minister of the Interior), parliaments remained operational and active. Thus, the crisis of the health and economic systems did not develop into a parliamentary crisis.

The legal structure of data protection in South-East Europe is different. In the four South-East European states that are members of the EU (**Bulgaria**, **Romania**, **Croatia** and **Slovenia**), the GDPR (basic data protection regulation) has been in force since May 2018. Most other countries in the region, whether or not they have already been granted EU candidate status, are in a process of gradual alignment of national legislation to the EU acquis communautaire. Most of their national data protection laws are therefore modernized and adapted to the GDPR, such as the Data Protection Law in Kosovo, which entered into force in March 2019. The same applies to the **Republic of Moldova**: although not an accession candidate or even a candidate country, at the end of 2018 it had partially transposed the GDPR into its national legal system. With regard to the protection of the data of people suffering from COVID-19, neither **Moldova** nor **Romania** have yet seriously debated systematic misinterpretation or violations of the GDPR. States are allowed to take emergency measures under their internal law which further regulate (i.e. restrict) the means of communication, but according to current knowledge this has not yet been used.

In **Romania** and the Republic of Moldova, the legislator did not lay down specific rules for the processing of health data that were specific to the COVID 19 pandemic. At the same time, however, employers were required to carry out health checks on employees (temperature measurement with thermometers). The same applies when entering a supermarket, which does not seem to be problematic in the light of the GDPR: this is not data that would make a person identifiable. At the same time, it is too early to assess the systemic impact of all newly introduced special rules.

Practical implementation

Compared with some Asian countries (see II. below), corona tracing apps were used late in South-East Europe. Data protection concerns of the population were partly addressed, as we know from the debate on the type of data storage (centralized vs. decentralized) in Germany. In **Poland**, for example, before using the Bluetooth-based app "ProteGO", the authorities published its source code to obtain opinions from IT experts and to dispel concerns among the population. These are, justified or unjustified, still very pronounced in Europe. For example, a survey in **Slovenia** in mid-July showed that only about a quarter of the population would voluntarily install a tracing app on their mobile phones. The Slovenian Parliament adopted a law at the beginning of July which allows the use of an app in **Slovenia**. However, Prime Minister Jansa called for a uniform EU-wide app, which should be mandatory for all citizens..[12]

However, a European or at least EU-wide uniform technical solution for the use of "corona tracing apps" (CTA) is still not in sight. Accordingly, in addition to Hungary, the South-East European EU member states **Croatia** and **Romania**, for example, now have their own plans to develop a national app and launch it shortly, although such apps are not yet in use (at of the end of July 2020).

In the meantime, however, there are now first experiences with Tracing Apps in some other South-East European countries. In the EU member state **Bulgaria**, for example, the app "ViruSafe" has been in use since the beginning of April 2020. When registering, the user has to enter his ID data; the data is stored in a central register..[13] According to initial reports, however, this app is only used by a few Bulgarians. Since 13 April 2020, citizens of the EU candidate country **Northern Macedonia** have been able to use the app "StopKorona!"..[14] This app is Bluetooth-based, and the developers base their programming on the

"TraceTogether App" used in Singapore. Data is stored for a maximum of 14 days on the mobile smartphones of those who have voluntarily downloaded and installed the app. In addition, **Macedonian** users have the option to voluntarily send data to the Ministry of Health.

In **Croatia**, the road to the use of an app was somewhat longer: first, an amendment to the Telecommunications Act was discussed which would have allowed the authorities to geolocate. However, at the end of July, an app based on Bluetooth technology was approved by the state regulatory authority: The tracing app "Stop COVID 19" relies on decentralized data storage and does not transmit location data..[15]

It is expected that other countries in the region will soon follow and use similar apps based on decentralized data storage, including Serbia, which has already largely harmonized its data protection legislation with EU law..[16]

Some South-East European countries have adopted other - more worrying - ways to contain the further spread of the pandemic: **Montenegro** briefly published a list of all quarantined citizens. State authorities in **Bosnia-Herzegovina** published the names of all those who had not respected self-isolation at the end of March, despite the fact that the Bosnian data protection agencies had declared this practice unlawful..[17]

In the **Republic of Moldova**, during the pandemic or health emergency, an app was developed for only a small group of people with tuberculosis so that they could receive remote treatment as a risk group. However, no Moldovan government authority has yet announced the development of a CTA. Even IT experts from the private sector are not yet working on it, but rather on aspects of facilitating the treatment of corona patients.

In **Romania**, the government announced relatively late, in June 2020, that a military hospital was developing such an app in cooperation with a private company. However, the Romanian CTA will only be operational in a year's time, according to the competent authority. There is currently no major debate on the architecture of the app. All that is known at this stage is that, similarly to countries already using such an app, the CTA will notify users as soon as they approach a corona hotspot, which should also be done by using Bluetooth. In addition, this application should enable health authorities to locate and act more quickly on the hotspots. The data will be sent in encrypted form to a public authority. Because of the encryption, the government will not have access to personalized data. It remains questionable, however, whether such an app will be able to fulfil its purpose reasonably only in a year's time.

Legal problems

With regard to data protection, it must be noted that, despite national regulations in South-Eastern Europe formally complying with the requirements of the GDPR, there is still a long way to go to achieve effective protection of personal data, which is also internalized and respected by all actors: the publication of lists of names of infected persons in **Montenegro** (the data published on the Internet have now been deleted) and quarantine violations (**Bosnia-Herzegovina**) are only the most serious violations. There have been isolated cases of such publications in other south-east European countries, e.g. when the Moldovan President publicly announced the full name of the first infected Moldovan citizen, which was a clear breach of Moldovan data protection law.

Conclusion and perspectives

The legislative monopoly of the parliaments, derived from the principle of separation of powers enshrined in the constitutions of all countries of South-Eastern Europe, has always been respected. In some countries, special regulations relating to the pandemic were adopted by simple laws, leaving the respective (emergency) authority a certain amount of leeway as to how they were to be put into practice, including, for example, the establishment of a list of "safe countries of origin" upon entry into the national territory.

It is still too early for a final evaluation of technical applications in South-Eastern Europe for tracking corona infections using smartphones. Many countries in the region do not yet have an app in place. However, data protection law aspects are mainly considered, which is why solutions with decentralized data storage predominate in practice. Court investigations of these apps are not yet known. However, the fact that fundamental rights considerations are observed in practice by the courts even in times of the Corona pandemic has been shown by the examination and rejection of curfews by constitutional courts in the region.[18]

II. Asia

Gisela Elsner, Aishwarya Natarajan

In Asia, a total of 10 to 15 countries currently use or are developing different contact tracing technologies to contain and control the pandemic, mostly in the form of apps that work via smartphones. This paper highlights three Asian countries, **Singapore**, **South Korea** and India, to illustrate the broad regional trends in the use of contact tracing apps to combat the COVID 19 pandemic.

Legal framework

All three countries are constitutional democracies according to their constitutional texts. The constitutions contain emergency provisions, but these have not been used to combat the COVID 19 pandemic.

Singapore adopted a special law in April 2020, the *COVID-19 Temporary Measures Act 2020* (CTMA). At the beginning of the outbreak, the **Singapore** government relied on the *Infectious Diseases Act* and the *Immigration Act* to respond to the health crisis. The CTMA gave it wide discretionary powers to issue investigation orders.[19]

The **Indian** government relied on the *National Disaster Management Act* (NDMA) as the legal basis for supporting government initiatives to combat the pandemic. The government used its authority to issue guidelines and instructions under the NDMA to legitimize the establishment of the *Aarogya-Setu*-App and promote its use.[20] At the beginning of May, the Ministry of the Interior declared the use of the *Aarogya-Setu*-App binding for workers in the private and public sectors. It also called on local authorities to ensure 100% coverage of the app in areas with access and exit restrictions.[21]

In February 2020, the National Assembly of **South Korea** adopted amendments to the *Infectious Disease Control and Prevention Act* (IDCP), the *Quarantine Act* and the *Medical Service Act*. The IDCP provides a basis of legitimacy for the holding and processing of personal data of infected persons and enables the authorities to access recordings from security cameras, credit card records and GPS data from vehicles and mobile phones in order to trace the movement paths of COVID-19 infected persons.[22]

Practical implementation

In spring, the **Singapore** government asked the population to install the TraceTogether app.[23] Launched in March as one of the first of its kind in the region, it works through mutual smartphone recognition via Bluetooth, with contacts stored locally on the device. In case of infection, the smartphone user decides whether the health authorities will have access to the stored contact data. The use of this app is currently still voluntary.[24] In addition, the *SafeEntry* app, which functions as a national digital check-in system and *must* be used at all workstations, was also introduced in Singapore.[25] Since the beginning of July, portable tracking devices have also been distributed to residents, initially mainly to older citizens who do not have suitable smartphones that would allow them to use the *TraceTogether* app.[26]

In **India**, the government launched the smartphone app called *Aarogya Setu* to enable contact tracking. The data is stored on a central server of the government after allocation of an identification number. The scope of the stored data, which is intended to help identify the user, is wider than in Singapore. When registering, the app transmits the current GPS location, full name, telephone number, age and sex, occupation and information on the countries visited in the last 30 days to the server. In addition, the smartphones interact via Bluetooth and the corresponding data is stored locally on the devices. The application continuously stores (at 15-minute intervals) the GPS location data of the smartphone and provides for regular self-examination of symptoms by the users, the results of which, including geolocation data, are transmitted to the server when infection is suspected. Furthermore, the corresponding user agreement ensures the anonymization of the data.[27]

In the case of **South Korea**, the approach to dealing with the pandemic differs from that of the two countries described. No specific contact tracing application has yet been introduced. However, following the outbreak of MERS in 2015, South Korea has already adapted its health sector legislation to deal more effectively with public health crises caused by infectious diseases.[28] The country has introduced new laws to allow health authority investigators to access personal data. These rules allow for exceptions under the South Korean *Personal Information Protection Act* if there is a "public interest" in doing so, including for the purpose of investigating the spread of infectious diseases. These exceptions have empowered the authorities to access detailed personal data, including, for example, credit card transactions at banks or mobile phone location data at telecommunications operators. The analysis of the combination of such data with video footage from surveillance cameras has been used for early identification of corona cases.[29]

While the legislative approach to combating the pandemic is different in the three countries, there is real common ground in the approach to the use of contact tracing apps. Both Singapore and India have found ways to encourage employers to use contact tracing apps. The recent directive issued by the **Indian** Ministry of the Interior contains a provision requiring employers to "ensure that Aarogya Setu is installed by all workers with compatible mobile phones". The mandate is to be fulfilled by the employer "to the best of his ability".[30] In the case of **Singapore**, the *SafeEntry* app must be used at all workstations. Industry regulators such as the *Monetary Authority of Singapore* have emphasized that employers are responsible for compliance in this respect. Both Aarogya Setu and SafeEntry collect sensitive personal data such as name, personal identification number and mobile phone number.[31] These measures transfer the responsibility for using the app to the employer and make it a prerequisite for most employees in the formal sector to resume work in the workplace. In the case of **South Korea**, the invasive nature of the contact tracing procedure theoretically provides the government with ample opportunity to access personal data of citizens not related to Corona.

Legal problems

Some experts in **Singapore** have called for mandatory use of the app.[32] - at a time when the government continues to assure that the use of the TraceTogether app will not be made mandatory..[33] Opposition parties have called on the government to be careful about the privacy of Singaporeans..[34] In **India**, the compulsory use of the Aarogya-Setu app has provoked strong criticism from experts such as the former Supreme Court Judge BN Srikrishna, who found that such a move would be illegal as there is no legal basis for it..[35] Meanwhile, the Indian judiciary has taken the prima facie view that in these unprecedented times it may not be appropriate to interfere with government orders..[36] In the case of **South Korea**, the government has also been severely criticized for passing on information about infected people, particularly in the case of a COVID 19 outbreak in a district frequented by the LGBTQ scene..[37]

Conclusion and perspectives

Developments in the three countries described here reflect the wider context and also the race to use contact tracing apps in the region and beyond. This trend naturally raises a number of privacy and data protection issues. At the same time, it offers governments the opportunity to enhance their legitimacy by taking into account the requirements of the substantive rule of law when using digital contact tracing technologies, even in times of pandemic. Beyond the worldwide cultural differences in the concept of data protection, the debate has also put the spotlight on these countries in terms of how they deal with their citizens' right to privacy. It has become clear that their protection is essential for citizens to be able to trust these apps, modern technologies as a whole and also their own governance.

III. Latin America

Marie-Christine Fuchs, Magdalena Schaffler

Latin America is currently at the peak of the first pandemic wave and represents the new global epicentre of the coronavirus. Case numbers are expected to increase steadily until September. As the virus has so far not been stopped even by extreme measures restricting civil liberties, the discussion on the use of corona tracing and tracking apps also started in Latin America somewhat later than in Asia and Europe. Although there are numerous providers of different software, not a single country in the region has yet introduced a compulsory surveillance system for mobile phones. Data protection considerations have also been neglected.

Legal framework

There is no unified data protection law comparable to the GDPR in Latin America. As early as the 1990s, a few data protection regulations found their way into constitutions and national legal systems, for example in **Peru**..[38] **Chile** has regulated the protection of personal data since 1999..[39] However, the scant case law on this is highly controversial..[40] In **Colombia**, too, current laws on the protection of personal data do not yet provide for a general "right to forget" (right to delete data) or to establish data protection bodies..[41] **Mexico**, on the other hand, has one of the most comprehensive data protection legislations.[42] in the region with the Federal Personal Data Protection Act, which came into force in 2010. In addition to detailed regulations on the collection, use, transmission and storage of data, the law also regulates rights of access, correction, objection and deletion. The Mexican data protection authority, *Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos*

Personales, enjoys a reputation as one of the most active data protection institutions in Latin America.[43] However, even in countries with data protection regulations, effective protection has so far largely failed to be implemented administratively.[44]

However, the adoption of the EU 2018 GDPR has nevertheless led to a wave of reforms in data protection law in Latin America as well, and many legally established rules for the protection of personal data have been adapted to the standards laid down in the EU regulation. Some countries that did not have their own data protection laws until then, such as **Brazil**[45], also followed suit. However, the level of protection is still not as high as in the EU.

Practical implementation

Due to a rather lax handling of personal data and a widespread acceptance or acceptance by the population of private as well as governmental mobile phone surveillance, it is not surprising that the recommendation to use corona tracking apps as a tool to contain the pandemic does neither cause sensation nor too much concern among the Latin American population. Only sporadically the use of such apps is questioned by representatives of civil society, NGOs and scientists and legal grey areas are discussed. Critics of such apps fear in particular that the data collected through the installation of the software, especially health data, could not be managed by governments in accordance with data protection regulations or even be used for other purposes, for example for election campaign purposes or other manipulation of the own population in the worst case.[46]

Unimpressed by this, the Latin American governments extensively praised corona tracking apps as a promising digital medium against the spread of the coronavirus, especially in the period between May and June 2020. This was not only done on radio and television, but also automatically in Colombia, for example by an announcement before every telephone call.[47] There is still no legal obligation to use tracking apps in Latin America; the use of tracking apps is still voluntary.

In addition to some apps covering the whole region, such as the "David19" app offered by the Inter-American Development Bank,[48] you can find both national and local comparable and often competing applications of better and worse quality in the individual countries.[49] The providers and operators of these corona tracking apps are all government institutions, usually the ministries of health. In the meantime, it is also the employers, whether public or private, who promote the use of various corona tracking apps or comparable digital questionnaires among the Latin American population.

Legal problems

The voluntary use of corona tracking apps gives the impression to the outside world that state bodies take their duty to respect rights such as the protection of personal data seriously. However, if one takes a closer look at the data protection declarations and terms of use of individual software in the region, it quickly becomes clear that this is not always the case. For example, the **Mexican** Ministry of Health, as the official provider of the Mexican COVID-19MX app[50], reserves the right to make any updates to data protection regulations without prior notice and to disclose the data collected with the app to third parties without specific reasons. It explicitly excludes itself from civil and criminal liability for any misuse of data.[51]

Colombia's information policy on the protection of personal data at "CoronApp" is also questionable. According to Colombia's data protection law[52], the unrestricted disclosure of personal data in medical emergencies is permitted even without the consent of the person concerned. According to the Colombian government, this also includes "sanitary

emergencies"..[53] Although the terms of use of the Corona App refer to the deletion of the data after the pandemic has abated, this is only the case if the collected data does not have to be kept for historical, scientific or statistical purposes..[54] This opening clause could be used as a pretext for unlimited data retention.

The Chilean "CoronApp"'s compliance with data protection legislation also raises at least some doubts, due to imprecise wording in the data protection provisions, as to the lawfulness of processing and transferring collected data to third parties. It is still unclear whether this requires the explicit consent of the users or whether the Chilean Ministry of Health is given a free hand in this respect..[55] An attempt is made to legitimize the unlimited data collection intention by means of the app with the indications that the data can be used for historical, statistical, scientific and study or research purposes or that the data can be stored for an unlimited period of time, but at least up to 15 years..[56]

Conclusions and perspectives

Despite widespread mistrust of state institutions among the population, the apps offered are for the most part installed without critical scrutiny and are also actively used, especially in Latin America's mega-cities. Despite critical voices regarding the danger to data protection, Latin Americans are still not fully aware of their basic rights to the protection of personal data. There is a widespread perception that the voluntary use of apps reduces the effectiveness of these digital tools in curbing the pandemic..[57] Moreover, many citizens on this continent, which is particularly marked by social inequality and precarious living conditions, do not even know how they will be able to feed their families tomorrow due to the economic crisis triggered or intensified by the pandemic. Concerns about data protection are receding. In Latin American countries, where a large part of the population does not even have access to drinking water, let alone to smartphones,[58] widespread success in containing the pandemic through the use of corona apps is questionable. In contrast to highly developed countries in Asia and Europe, the basic structural conditions for nationwide data monitoring and an associated positive effect on the containment of infection rates do not exist across the board.

IV. The Middle East and North Africa

Dr. Malte Gaier, Anja Finke

The first corona warning apps were developed comparatively early in the Maghreb and Gulf states. Especially in these countries, often characterized by a powerful executive and often inadequate data protection regulations, there is a great danger that without a clear legal situation and effective monitoring bodies, corona warning apps could also be used for state monitoring and the restriction of individual freedoms.

Legal framework

There is currently no specific national data protection legislation in **Saudi Arabia**, but Sharia principles and other sectoral laws in the electronic communications sector aim to protect the privacy and personal data of individuals..[59]

The **United Arab Emirates** also have neither a national data protection law nor a national data protection authority. However, *Federal Law No. 2* (known as the "Health Data Act") regulates the use of information technologies in the health care system. This is the first federal law to deal directly with the principles of data protection.

In addition, *Federal Law No. 5 on Combating Cybercrime* prohibits the disclosure of information that has been obtained illegally by electronic means. However, it is doubtful to what extent these laws regulate state intervention in practice.

The **Kingdom of Bahrain** introduced a far-reaching data protection law in 2019 with *Law No. 30* on the protection of personal data.

Morocco also has regulations on the protection of personal data. These include *Law 69-99 on archives, Law 31-13 on the right of access to information* and *Law 09-08 on the protection of personal data*.

Tunisia occupies a special position from a data protection point of view: Data protection law was enshrined in the Constitution as early as 2014 and the protection of privacy was placed at the top of the list of rights and freedoms to be guaranteed. In March 2018, a new draft law on the protection of personal data in line with the new EU data protection basic regulation was submitted to Parliament, but the law has not yet been adopted. Meanwhile, *Law No 2004-63 of 27 July 2004* regulates the protection of personal data, which is considered obsolete as regards new technologies.

In **Jordan**, the right to privacy is enshrined in the Constitution, but there is currently neither a specific data protection law nor a data protection authority that could regulate data processing through a corona app.

In **Lebanon**, a new data protection law was introduced in 2018, but it falls far short of its counterparts in the region, and even less so of the standards set by the DPA, and does not sufficiently guarantee the protection of personal data.[60]

Practical implementation

In the Gulf States, enormous resources have been allocated to the digitalization of infrastructure over the last ten years: New partnerships with big tech companies have been established, legislation has been adapted and skilled workers have been trained. While the historically low oil prices and the COVID 19 pandemic are shaking up the Gulf economy, the latter is undoubtedly also the biggest acid test yet for the long-term digitalization efforts in the health sector.

The app "Tabaud" ("Distancing") was published in **Saudi Arabia** in early June. The smartphone application was developed by the National Information Center of the Saudi Arabian Authority for Data and Artificial Intelligence in close cooperation with the Ministry of Health as a warning system and to identify chains of infection. It informs users of the app if they have had contact with a person who has tested positive for COVID-19 in the last 14 days. For this purpose, *Tabaud* records which smartphones have come close to each other and exchanges randomly generated crypto-keys via Bluetooth. This has the advantage that neither geodata nor location information is evaluated. The installation and use of the application is free and voluntary.

When the pandemic broke out, the **United Arab Emirates** (UAE) also benefited considerably from its systematic promotion of digitalization in recent years. Against the background of the National Innovation Strategy, the Artificial Intelligence Strategy and the "Blockchain Strategy 2021", the transition to distance learning and distance education was smooth and

rapid. Already in April 2020, the UAE Ministry of Health initiated the TraceCovid app with the aim of detecting infection chains at an early stage and automating and accelerating the notification process. The mobile application exchanges an encrypted *Secure Tracing Identifier* (STI) with other devices on which the app is installed. This consists of an anonymized date and time stamp, which is stored locally on the devices for three weeks. If a user tests positive for the virus, the STI is uploaded to a central server.

At the same time, the Ministry of Health introduced the smartphone application "Stay-Home". The app enables the Ministry to stay informed about the whereabouts of people in mandatory home quarantine. To do this, the user must allow the app to access the camera, location, audio and calls.

At the end of April, these functions were finally combined in the "Alhosn" app, which also allows users to receive the test results on their smartphones. In most cases, the app is still used on a voluntary basis. However, people who have tested positive for the corona virus in the UAE and those who have come into close contact with infected persons will have to wear an electronic bracelet which is connected to the *Alhosn* app. Those who do not wear the electronic bracelet risk 6 months imprisonment and/or a fine of up to 100.000 Dirham (24.260 Euro) for repeated violation.

The **Kingdom of Bahrain**, in turn, recently made negative headlines with its "BeAware Bahrain" warning app. According to a report published by *Amnesty International*, the app is one of the most invasive applications for detecting chains of infection. A Bahraini ID number is required to register and use the application. The app performs near-live tracking of users' locations and uploads the GPS coordinates to a central server. This is to identify risk contacts of the last 14 days. BeAware Bahrain was also linked to a nationwide live TV show called " Are You at Home?", where prizes were awarded to people who stayed home during Ramadan. Participation in the raffle was initially mandatory, but was then offered as an additional voluntary feature.

The Bahraini warning app can also be paired with a Bluetooth bracelet to ensure that users respect quarantine regulations. For this purpose, the location data is uploaded to a central server every 10 minutes. Wearing the bracelet is mandatory for all persons registered for home quarantine. Violation of this rule may result in a prison sentence of at least three months and/or a fine of between 1,000 and 10,000 BD (approx. 2,345 EUR - 23,500 EUR).

A similarly early response can be observed in North Africa. Despite the comparatively small number of cases, the governments of the Maghreb countries reacted early and comprehensively to contain the novel corona virus, given the often inadequate health care. In addition to travel and contact bans and strict curfews, warning apps were used early on.

In **Morocco**, as part of the national strategy to combat the corona pandemic, a multidisciplinary team from the Ministry of Health, the Ministry of the Interior, the National Regulatory Authority for Telecommunications and the Agency for Digital Development developed the smartphone application "Wiqaytna" ("Protection") in cooperation with Moroccan companies and start-ups. Since 1 June, the Moroccan population has been able to download the app free of charge and thus be notified if there has been a risk contact with other users in the last 21 days. Each time another user of the app encounters another user, a random, anonymous and encrypted code is recorded via Bluetooth and stored locally on the devices. At the end of the 21 days, the information is automatically deleted.

If a user tests positive for the virus, he will be asked to upload the encounter data to a central database. Under no circumstances should the identity of the infected person, the place or time of the encounter be revealed.

In **Tunisia**, the smartphone application "E7mi" ("Protect") has been available for download since 19 May. The application was developed by the Tunisian start-up Wizzlabs. As soon as a user of the app has tested positive, the Emerging Diseases Observatory notifies other users who have come into contact with this person in the last 14 days and then initiates the necessary follow-up measures. The app also uses Bluetooth to record contact between users, but stores and processes the encrypted data on a central server in Tunisia rather than on the device. For registration, the App requires only the user's telephone number, so that in the event of a proven infection, neither the identity of the infected person nor the place and time of the encounter are revealed. The use of E7mi is currently voluntary. However, the Tunisian Ministry of Health announced that the app could become mandatory in public places if the installation rate remains too low. The Corona Warning App is under the control of the National Authority for the Protection of Personal Data.

In the countries around the east coast of the Mediterranean, after a first slow return to normality, a second wave of the corona virus seems to be on the horizon during July. Unlike in the Gulf and Maghreb countries, there is currently no clear trend towards digitalization in the Levant to track infection chains. However, especially in this region marked by conflicts and political and socio-economic instability, it is important to keep the pandemic in check to prevent further destabilization.

So far, only **Jordan** has launched a voluntary Corona warning app for contact tracing on 21 May. The "Aman" ("Security") application was developed by the "COVID-19 Jotech Community", a group of technically skilled volunteers, on behalf of the Jordanian Ministry of Health. According to its developers, the application is described as a "privacy app for detecting exposure to the corona virus", which sends automatic alerts to users in case of a risk contact. In this case, the app provides users with instructions on how to quarantine at home and how to contact the competent authorities. Aman follows a decentralized approach to data storage, according to which the data is stored for 14 days on the users' devices.

In **Lebanon**, COVID-19 cases have so far been recorded in the same way. At an early stage, extensive contact bans, curfews, border closures and compulsory masks were introduced. A call centre of the Epidemiological Surveillance Unit of the Ministry of Health and the Rafik Hariri University Hospital in Beirut contacts people who have tested positive in order to trace and notify potential contact persons with an increased risk of infection. However, on 16 July 2020, the Lebanese Ministry of Health announced that it would work with experts from the American University of Beirut and the company Tedmob to introduce the corona tracing app "Ma3an".

A particularly worrying implementation took place in war-torn neighbouring Syria. According to the US company Lookout, Syrian authorities allegedly used encrypted malware via the prevention app "Covid19" to collect user data. The spyware is said to have enabled the regime to record the location, messages, pictures, videos and contacts of users, thus identifying and locating government critics.

Legal problems

One of the main problems is the absence of legal regulation in many of the countries studied. But even where data protection regulations exist, the implementation of data protection is doubtful. An example is Morocco: Despite the existing data protection laws, it is questionable to what extent sufficient data protection is ensured in the context of the corona pandemic. For example, Law 09-08 on the protection of personal data in particular denies the protection of such data that are collected and processed in the interest of national defense, internal or external security of the state and the prevention or combating of crime. Should the fight against the pandemic also fall under this, which is still unclear, data protection could be undermined.

Conclusions and perspectives

Many countries in the Middle East and North Africa either do not currently have specific data protection laws, or have laws that are outdated and therefore do not address today's data processing and data retention risks. Due to this often insufficient protection of personal data and the lack of transparency regarding the type and duration of data retention, corona warning apps could therefore be used for data misuse and, in the worst case, for state surveillance. Effective and independent monitoring bodies and legal channels would also have to enable citizens to take action against potential intrusion into their privacy and other individual freedoms. However, in the MENA region, whose countries are, with a few exceptions, characterized by over-powerful executives, the necessary counterbalances in the form of strong and capable parliaments and independent courts are often lacking.

V. Sub-Saharan Africa

Arne Wulff

In contrast to Europe or Asia, the issue of corona warning apps on smartphones in sub-Saharan Africa only plays a minor role. Only a few of the 49 countries are addressing the issue to any significant extent. The free provision of an app on mobile phones, as is the case in Germany, for example, is still a long way off. Instead, country-specific solutions are developing in various African countries. They are united in the goal of preventing infections by timely warnings or identifying infected persons in time. However, the legal foundations in the area of data protection law are only rudimentary; only a good handful of states have created a corresponding legal framework. For this reason, only an overview can be given here.

Practical implementation

The app "Fuata" was developed in **Kenya**, which is the closest to the app developed in Germany. Everyone who downloads this app to their smartphone receives a personal identification number (ID). The smartphones on which this app is installed communicate with each other via Bluetooth and record the ID of the other device for a period of 21 to 30 days. If one of them tests positive for Corona during this period, it will be possible to track which other people using the app have been in their vicinity and warn and test them accordingly. Privacy is protected by the fact that no GPS geolocation is used and personal data of the App user cannot be accessed by authorities. However, the developer still lacks the means to offer the app. He hopes for the support of major Kenyan mobile phone providers such as *Safaricom*.

A similar app, which uses GPS data in addition to Bluetooth, is currently being developed in **Uganda**. **Rwanda** also wants to go down this path. The "Rwanda Utilities Regulatory Authority" has commissioned the development of an app that enables the tracking of people who have had contact with corona infected people. In both cases, movement profiles are used to identify the infected and vulnerable persons. The data can also be used to control quarantine regulations and "social distancing".

For technical reasons, the use of the apps requires a smartphone. However, the level of distribution of these devices in sub-Saharan Africa is still quite low. Although the density of mobile phones is now relatively high (e.g. 97 mobile phones per 100 inhabitants in Kenya, 167 per 100 in South Africa, but also only 59 per 100 in Ethiopia and 44 per 100 in Angola) this does not apply to smartphones, however. While 79 % of the population in Germany have a smartphone, this figure is only 35.5 % in South Africa, 20.9 % in Kenya, 15.6 % in Uganda and 13 % in Nigeria (Newzoo Global Mobile Market Report 2018). Thus, the benefits of a corona warning app are very limited - after all, the degree of its effectiveness depends on the number of users.

A **South African** start-up is therefore taking a different approach. The company "Automatech" uses a small device instead of smartphones, which can document the contact between infected persons with the help of its own software. The device, which costs about 15 EURO, has already been ordered by larger companies in order to be able to better warn their staff equipped with it of infections caused by contacts at work. Unlike most apps, the device does not detect where you are, but only who you have been in contact with, if the person in question is also equipped with such a device. This makes it impossible for the provider, the government or hackers to determine the identity of the user or to create a movement profile - a fact that is particularly important in terms of personal data protection.

Legal problems

There is much to suggest that concern about the security of personal data is one of the reasons for the low demand for a "tracing app" in sub-Saharan Africa. It is true that all African states have joined the International Covenant on Civil and Political Rights (ICCPR) of 1966. Among other things, it protects the personal freedom of all people. However, the Covenant has not yet been expanded to include a legally binding instrument for data protection and privacy, as Germany, among others, has been calling for since 2013. It is true that 24 African states have passed laws and regulations to protect personal data. These include 14 states that have signed the African Union's "Convention on Cyber Security and Data Protection". In it, the states undertake, among other things, to establish a legal framework in their countries for the protection of personal data. In fact, only six countries have ratified the Convention (**Senegal**, **Namibia**, **Mauritius**, **Guinea**, **Ghana** and **Rwanda**). In most cases, however, implementation is lacking even where nation-state regulations for data protection have been created. For example, no competent state institutions and bodies have yet been established to ensure protection, or data protection officers appointed to which citizens could turn. In addition, there are fears on the part of smartphone users that downloading a corona warning app will expose them even more to the already intensive state control. In **Zimbabwe**, for example, there is a lively debate on how it has been possible for the authorities to trace people who have left their quarantine without authorization. It is suspected that movement profiles were created from their mobile phone data, which would not be legally permissible.

Conclusions and perspectives

As long as the spread of smartphones is low in many African countries and people are worried that corona warning apps will be subject to government control rather than personal protection due to a lack of data protection and authoritarian systems, acceptance of these digital assistants will remain low. Curiously, this is even more true in times of the COVID 19 pandemic: in many countries, state security forces are already abusing the precarious situation of the population. The population does not want to encourage this by downloading an app.

VI. Résumé

Pavel Usvatov, Gisela Elsner, Marie-Christine Fuchs

Right at the beginning of the pandemic, the governments of almost all countries in the regions studied declared the state of emergency that is constitutionally most permissible in their countries, which in many cases gave the already very powerful executive even more powers. At the same time, however, there are also fears, not without good reason, that the poorly developed health systems in many places in the regions could collapse quickly in view of rapidly rising case numbers. Many governments have therefore reacted by issuing decrees that contain worryingly extensive restrictions on freedom, such as quarantine measures lasting several months, strict curfews or border closures. In many places it is difficult to judge whether the measures are intended solely to protect health or whether they are intended to encourage the expansion of state surveillance under this guise.

The possibilities for comprehensive and accurate surveillance of the population, linked to the development and use of corona tracking apps, raises a number of privacy and data protection issues. In addition, the general questions arise as to whether and how the principles of the rule of law can be observed and the protection of civil liberties guaranteed under these circumstances. At the same time, governments have the opportunity to enhance their legitimacy by taking into account the requirements of the substantive rule of law when using digital contact tracing technologies and ensuring effective protection of citizens' rights, even in times of pandemics.

Beyond the social and political differences that exist worldwide with regard to the concept of data protection, the debate has also brought the states presented here into the limelight with regard to their handling of their citizens' right to privacy. International and national human rights organizations and representatives of civil society worldwide are increasingly demanding that the operators of corona warning apps must limit the collection of data to the minimum necessary in accordance with the principle of proportionality and guarantee secure and anonymous storage. Any data collection must be limited to pandemic containment and should not be used for other purposes, in particular for law enforcement, national security or immigration control purposes. It must also be ensured that data is not disclosed for commercial use. Particular attention must also be paid to guaranteeing the voluntary use of the apps. For this purpose, it should be ensured that there is no de facto obligation to use the apps by making them a prerequisite for social participation. Finally, citizens must not be introduced to and accustomed to permanent surveillance. All this is not yet guaranteed at present.

From a practical perspective, the effectiveness of apps in containing the pandemic or generating reliable data remains questionable if they are not used by a large majority of the population. As states begin to relax other restrictions, governments are increasingly looking for ways to promote the use of such apps. Therefore, addressing privacy concerns should be part of the strategy to slow down the pandemic and not be dismissed as a luxury. In these circumstances, many difficult questions related to this issue remain unanswered, including how information can be collected and secured in a privacy-compliant manner, who has access to the data, what legal, organizational and technical safeguards can be put in place to minimize the risks of data exchange and misuse. A key aspect is also how states deal with the collection of data after the end of the pandemic: here there are declarations of intent by governments to then delete the data and not to continue collecting it. However, there is no legal regulation on this issue that contains corresponding obligations. But it is now becoming increasingly clear that the protection of personal data is of central importance for the citizens of most countries, so that they can trust these apps, modern technologies in general and their own governance.

The use of modern technology will be essential in combating this and similar pandemics. The ultimate question should therefore be: Will the experience gained now make it possible in future to normalize the surveillance behaviour of states and companies in an orderly legal manner while respecting civil rights? In view of the still underdeveloped legal bases for the use of such technologies in many places, it remains unclear at present what mechanisms will emerge in the regions of the world under investigation to protect against invasion of privacy, comprehensive surveillance and possible prosecution of certain groups of people. However, awareness of these issues is growing - also outside Europe.

1 German Chancellor Angela Merkel in the podcast of 20 June 2020, www.bundesregierung.de/breg-de/themen/coronavirus/je-mehr-mitmachen-desto-groesser-der-nutzen-1762982.

2 By July 27th 2020, www.connect.de/news/corona-warn-app-download-zahlen-3200860.html.

3 Not to be confused with a "tra**ck**ing app", where a location is tracked, e.g. using GPS geodata or via the mobile phone network. *Tracing* is only about recording data on whether contact has taken place at all, not the location of the contact.

4 www.waz.de/politik/coronavirus-scheitert-die-tracking-app-fuer-den-kampf-gegen-die-pandemie-id228955653.html.

5 www.faz.net/aktuell/rhein-main/forscher-entdecken-sicherheitsluecke-bei-corona-apps-16812694.html.

6 For example, the transmission and storage of IP addresses in combination with anonymous data and the ID should allow conclusions to be drawn about the identity of the user, see „Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung" (FIfF) e.V., Analysis and constructive criticism of the official data protection impact assessment of the Corona Warning App, version 1.0 - 29 June 2020, p. 3, 5 et seq. Moreover, the IP itself and not the information behind it is already a personal date for the provider, BGH, VI ZR 135/13 - 16.05.2017, ECJ C-582/14 – 19.10.2016.

7 www.faz.net/aktuell/rhein-main/forscher-entdecken-sicherheitsluecke-bei-corona-apps-16812694.html.

8 For example, companies could make the use of the app a condition for access to business premises, www.datenschutz.rlp.de/de/aktuelles/detail/news/detail/News/kugelmann-pocht-auf-freiwilligkeit-der-corona-warn-app-sie-darf-nicht-zur-eintrittskarte-werden.

9 For a comprehensive presentation and further sources see *Joelle Grogan*, States of Emergency, verfassungsblog.de/states-of-emergency.

10 For example: "The greatest challenge since the Second World War" (Sebastian Kurz), www.rnd.de/politik/kurz-zu-coronavirus-grosste-herausforderung-seit-dem-zweiten-weltkrieg-O2KYRUWHPVHHBCRS5PBHJYNCBM.html; "We are at war" (Emmanuel Macron), www.spiegel.de/politik/ausland/coronavirus-in-frankreich-wir-sind-im-krieg-a-50b0dce2-6f7e-4cba-bda1-87fe05bfc7ca; summarising www.nzz.ch/feuilleton/corona-und-kriegsrhetorik-ld.1560145.

11 www.echr.coe.int/Documents/Convention_DEU.pdf.

12 www.euractiv.com/section/digital/news/slovenian-pm-calls-for-mandatory-coronavirus-app-against-commission-advice.

13 newseu.cgtn.com/news/2020-05-07/Why-COVID-19-contract-tracing-apps-are-causing-deep-division-in-Europe-Qhq5NSZgTm/index.html.

14 balkaninsight.com/2020/04/16/north-macedonia-leads-region-in-covid-19-tracing-app.

15 hr.n1info.com/English/NEWS/a530515/Croatia-presents-its-Stop-COVID-19-app.html.

16 cep.org.rs/en/blogs/covid-19-tracing-app-in-serbia.

17 www.balcanicaucaso.org/eng/Areas/Balkans/Not-just-apps-privacy-personal-data-and-COVID-19-in-the-western-Balkans-201814.

18 For example in Bosnia-Herzegovina, www.kas.de/de/web/rlpsee/laenderberichte/detail/-/content/ausgangssperre-verfassungswidrig.

19 verfassungsblog.de/singapores-legislative-approach-to-the-covid-19-public-health-emergency.

20 www.thehindubusinessline.com/news/why-legal-experts-think-aarogya-setu-app-cant-be-made-mandatory/article31621274.ece.

21 indianexpress.com/article/india/aarogya-setu-app-mandate-illegal-justice-b-n-srikrishna-6405535.

22 Art. 34 to (1)41 of the Act and Art. 76 to (3) of the IDPC.

23 hbr.org/2020/04/how-digital-contact-tracing-slowed-covid-19-in-east-asia.

24 www.channelnewsasia.com/news/singapore/covid19-trace-together-mobile-app-contact-tracing-coronavirus-12560616.

25 www.safeentry.gov.sg.

26 www.bbc.com/news/technology-53146360.

27 static.mygov.in/rest/s3fs-public/mygov_159051645651307401.pdf.

[28] Lee, Gyooho: Legitimacy and Constitutionality of Contact Tracing in Pandemic in the Republic of Korea (May 7th 2020), SSRN: ssrn.com/abstract=3594974 oder dx.doi.org/10.2139/ssrn.3594974.

[29] ibid.

[30] scroll.in/article/962687/by-making-employers-responsible-for-ensuring-aarogya-setu-use-state-has-outsourced-law-enforcement.

[31] www.gov.sg/article/digital-contact-tracing-tools-for-all-businesses-operating-during-circuit-breaker.

[32] www.todayonline.com/singapore/covid-19-governance-expert-says-tracetogether-should-be-mandatory-warns-potential-slippery.

[33] www.straitstimes.com/singapore/contact-tracing-device-will-not-track-location-and-people-can-use-tracetogether-if-they.

[34] Ibid.

[35] www.thehindubusinessline.com/news/why-legal-experts-think-aarogya-setu-app-cant-be-made-mandatory/article31621274.ece.

[36] www.thehindubusinessline.com/news/why-legal-experts-think-aarogya-setu-app-cant-be-made-mandatory/article31621274.ece.

[37] www.pri.org/stories/2020-05-22/south-korea-s-coronavirus-contact-tracing-puts-lgbtq-community-under-surveillance.

[38] Art. 2 par. 6 of the Constitutino of Peru from 1993: „Toda persona tiene derecho: A que los servicios informáticos, computarizado o no, públicos o privados, no suministren informaciones que afectan la intimidad personal y familiar".

[39] Law no. 19.628 of 1999, which focuses on the use of data by third parties. Monitoring mechanisms for proper compliance are missing in the law and the possibility to apply to the court for the deletion of data in case of unlawful use, as provided for in Article 16, has so far proved ineffective. See www.leychile.cl/Navegar?idNorma=141599.

[40] E.g. Corte Suprema de Chile, Rol N° 11256-2011, de 27 de enero de 2012, c. 6°.

[41] Law Nr. 1.581/2012 and Nr. 1.266/2008, decrees 1377/2013 and 886/2014.

[42] stcs.senado.gob.mx/docs/08.pdf.

[43] blogs.iadb.org/conocimiento-abierto/es/proteccion-de-datos-gdpr-america-latina.

[44] Herzog, Roman: Lateinamerika in der neuen Kommunikationswelt, in: Bodemer, Klaus / Gratius, Susanne (Hrsg.), Lateinamerika im internationalen System: Zwischen Regionalismus und Globalisierung, Springer 2003, p. 259.

[45] Until recently, Brazil lacked a specific law regulating data protection and even a definition of personal data. Instead, the country retained for years several sectoral laws containing general provisions on the protection of individuals and their data. The Consumer Protection Law, for example, provided some data protection rights to access and correct consumer data, and the Criminal Code provides the legal framework for processing personal data on the Internet. The LEI Nº 13.709, adopted in August 2018, entered into force at the beginning of 2020. Available at: www2.camara.leg.br/legin/fed/lei/2018/lei-13709-14-agosto-2018-787077-publicacaooriginal-156201-pl.html.

[46] www.ft.com/content/19d90308-6858-11ea-a3c9-1fe6fedcca75.

[47] www.elespectador.com/noticias/salud/funciona-o-no-la-coronapp.

[48] www.dw.com/es/david19-un-rastreador-digital-contra-la-covid-19-en-am%C3%A9rica-latina/a-53538288.

[49] web.karisma.org.co/coronapp-medellin-me-cuida-y-calivalle-corona-al-laboratorio-o-como-se-hackea-coronapp-sin-siquiera-intentarlo.

[50] socialtic.org/blog/analisis-app-covid19mx-resumen.

[51] socialtic.org/blog/analisis-app-covid19mx-resumen.

[52] Art. 10 of the Law Nr. 1.581/2012.

[53] sic.gov.co/sites/default/files/files/Nuestra_Entidad/Publicaciones/Compendio%202%20FINAL%20V%2012%20Dic20.pdf, S. 256.

[54] archive.org/details/informe-publico-tecnico-coron-app-v-170320-1/mode/2up.

[56] ciperchile.cl/2020/04/22/problemas-de-proteccion-de-los-datos-personales-de-la-aplicacion-coronapp.

[57] Cf. netzpolitik.org/2020/warum-freiwilliges-handy-tracking-nicht-funktioniert.

[58] The penetration of smartphones is estimated at around 69% in 2020, https://www.statista.com/statistics/218531/latin-american-smartphone-penetration-since-2008.

[59] Royal Decree No M/18: Law on Electronic Transactions; Royal Decree No M/17: Anti-Cyber-Crime Law.

[60] https://smex.org/an-ugly-new-data-protection-law-in-lebanon/.

Imprint

The authors

Dr. Pavel Usvatov was till August 2020 the coordinator of international Rule of Law programs of the Konrad-Adenauer-Stiftung.

Hartmut Rank, LL.M., MBA is the Head of the Rule of Law Program South East Europe of the Konrad-Adenauer- Stiftung.

Stanislav Splavnic, LL.M. is a research assistant at the Rule of Law Program South East Europe of the Konrad-Adenauer-Stiftung.

Gisela Elsner was till July 2020 the Head of the Rule of Law Program Asia of the Konrad-Adenauer-Stiftung.

Aishwarya Natarajan is a research assistant at the Rule of Law Program Asia of the Konrad-Adenauer-Stiftung.

Dr. Marie-Christine Fuchs, LL.M. is the Head of the Rule of Law Program Latin America of the Konrad-Adenauer-Stiftung.

Magdalena Schaffler is a project coordinator at the Rule of Law Program Latin America of the Konrad-Adenauer-Stiftung.

Dr. Malte Gaier is the acting director of the Rule of Law Program The Middle East / North Africa of the Konrad-Adenauer-Stiftung.

Anja Finke is a project coordinator at the Rule of Law Program The Middle East / North Africa of the Konrad-Adenauer-Stiftung.

Dr. Arne Wulff is the Head of the Rule of Law Program sub-Saharan-Africa (anglophone countries) of the Konrad-Adenauer-Stiftung.

Konrad-Adenauer-Stiftung e. V.

Dr. Pavel Usvatov
Legal and policy advisor Rule of Law Dialogue
Politics and consulting
T +49 30 / 26 996-3948
pavel.usvatov@kas.de

Address: Konrad-Adenauer-Stiftung, 10907 Berlin

Publisher: Konrad-Adenauer-Stiftung e. V. 2020, Berlin
Design: yellow too, Pasiek Horntrich GbR
Typesetting : Franziska Faehnrich

ISBN 978-3-95721-801-8

The text of this publication is licensed under the terms of "Creative Commons Attribution-ShareAlike 4.0 International", CC BY-SA 4.0 (available at: https://creativecommons.org/licenses/by-sa/4.0/legalcode.de).