No 435 / July 2021

Facts & Findings

KONRAD ADENAUER STIFTUNG

An Unfulfilled Promise

Data That Could Have Prevented Lockdowns

Pencho Kuzev

- No democratic country in the world can point to tangible positive effects from using tracing apps alone in the fight against corona.
- Comparisons with Asian countries are flawed and often do not correspond to the facts. Taiwan, for instance, does not use any kind of contact tracing app, while surveillance methods in South Korea contravene our legal system and democratic principles.
- The starting point determined by Apple and Google for the design of corona apps used worldwide makes contact tracing *virtually* impossible. The so-called decentralised approach based on data protection may protect people's privacy but does not provide any of the insights that public and academic health experts need.
- This pandemic has repeatedly confronted us with the *privacy paradox*. Democratically legitimated bodies are prohibited from using location data and central data storage for a clearly defined purpose, and with all legal guarantees.
- Unfortunately, the stance taken by data protection authorities in this pandemic is not exactly cohesive. But the legal framework is not to blame for this.

Table of Contents

Introduction

Data-based innovations could help to combat Covid-19 – many are still convinced of this today. But after more than one year of the pandemic, disenchantment is setting in: Germany is not satisfied with how the Corona-Warn-App has been implemented, nor has any other democratic country developed an alternative that could have had a positive effect on the occurrence of infection.

Contact tracing measures that live up to their name.

Immediately after the outbreak of the pandemic, several Asian countries implemented contact tracing tools – tracing apps – that lived up to their name. With the aid of corresponding QR codes, tokens (Singapore), check-in systems, surveillance cameras, GPS signals, traffic or credit card data (South Korea), conclusions could be drawn about when, where and by whom the virus was spread. However, there is no disputing that tools designed in this way have the potential for abuse, and result in a massive curtailment of fundamental rights.

In a *first* step, the following analysis documents the Federal Government's failed attempts to help contain the pandemic by using digital tools. The analysis also discusses what has not been implemented in the course of the pandemic so far. The roles played by relevant protagonists are analysed in retrospect. The *second* part carries out a critical appraisal of efforts taken in Great Britain and Australia. It discusses the role played by the market-leading operating systems of Google (Android) and Apple (iOS), and their influence on the global development of tracing apps. *Finally,* recommendations for action are provided for reconciling discourse on data protection policy in Germany.

Processing Personal Data to Serve Humanity

The right to protect personal data needs to be viewed with regard to its social function.

As early as the introduction of the General Data Protection Regulation (GDPR), the European legislator clarified that *"processing personal data should serve humanity".* The right to protect personal data is not an unconditional right; it needs to be viewed with regard to its social function and weighed against other basic rights while upholding the principle of proportionality".[1] In Germany, the impression has frequently been that data protection does not fulfil precisely this social function. The legal framework is not to blame for this, however.

One year after the outbreak of the pandemic, the controversial discussion about the role of the Corona-Warn-App continues. Many blame its limited effectiveness on the rigid implementation of data protection.[2] Data protection authorities are accused of being responsible for the ineffectiveness of the app, a criticism that was immediately rejected by prominent data protection specialists.[3]

The GDPR and the Fight Against the Pandemic – Not Mutually Exclusive

Despite the criticism levelled against the GDPR, it is a strong foundation for the social challenge of our age. The importance of data in a pandemic was already clear to see during the legislative process.[4]

The GDPR makes a direct reference to a pandemic situation.

If the processing of data is necessary to perform a task in the public interest or for exercising public authority, there needs to be a basis for it in Union or Member State law. Several legal provisions are considered as a legal basis for evaluating location data to combat the coronavirus: first and foremost, consent to the processing of data for the protection of vital interests or due to public interest in the area of public health. According to the GDPR, personal data should in principle only be processed for the vital interest of another person if no other legal basis can be invoked.[5] With some 15,000 new infections per day, this threshold has certainly been met. As regards necessity, the GDPR even makes direct reference to a pandemic situation: It states that "the processing (of data) may be necessary for humanitarian purposes, including the monitoring of epidemics and their spread".

Necessity of data usage

It is on this basis that in March 2020 the Federal Government took legal measures in an attempt to make the data-driven fight against the pandemic even more precise. However, efforts to make the work of health authorities easier were scotched due to fierce resistance in some social circles and in politics.[6] There was a lack of trust in the fact that tracking location data plays a role in contact tracing,[7] and that such a measure could well be in the spirit of the GDPR. For instance, the Federal Commissioner for Data Protection, Ulrich Kelber, deemed state-imposed access to the mobile phone data of infected persons to be more than problematic.[8] Besides the question of what legal basis should apply to such action, the proportionality of such an intervention must also be scrutinised. Such a measure can only be justified with the consent of the affected parties, as Kelber went on to explain in an interview with *Der Tagesspiegel*.

Infectious Diseases Protection Act and tracing location data

The Federal Ministry of Health submitted the draft of the Infectious Diseases Protection Act (IfSG) with clear reference to findings in Asian countries. This stated that: "International findings such as in the context of South Korean measures to contain Covid-19 demonstrate how the Infectious Diseases Protection Act and tracing location data can contribute towards contact tracing". The key part of the draft law was § 5 of the Infectious Diseases Protection Act (IfSG-E) with the heading "Epidemic Emergency Situation at the National Level, Power to Issue Ordinances".[9] The following regulations had to be deleted without substitution due to multiple objections. For the sake of completeness, we should note the following here:

> *"In the event of an epidemic situation (...) the competent authority may use technical means for the purpose of contact tracing to identify those who had contact with infected persons, provided it is ensured, based on epidemiological findings, that this is necessary to protect the population against exposure to serious communicable diseases. Under the conditions in Sentence 1, the competent authority may request any (...) service provider to provide available traffic data, the specific codes required for identifying the location of a mobile device and the (...) required data for those who have potentially had contact with infected persons.*[10] ***(...) The competent authorities may process personal data for this purpose (...)".***

To this end, the service provider merely needs to provide traffic data, specific codes as well as data that **enables contact to be made with data subjects.** The explanatory memorandum also clarifies that the authorisation **does not give competent authorities the right to gather any content data and communication content.**

This originally formulated regulation is entirely in accordance with the GDPR. It represented an authorisation for data processing according to Article 6 (1) sub-paragraph d and 2 as well as Article 9 (2) sub-paragraph i GDPR. Although the telephone location logs of mobile operators cannot provide 100 per cent accuracy, they can be useful in connection with other data for model analyses and contact tracing – as successfully practised in South Korea.

The Corona-Warn-App was Deliberately Not Developed as a Geo Tracking App

The starting point determined by Google and Apple for designing corona apps.

It may come as a surprise that location tracing was never a declared goal[11] when designing the Corona-Warn-App. Even if the Federal Government had wanted this, Apple and Google systems do not permit location tracing. This aspect receives scant attention in public debate. The starting point determined by Google and Apple for the design of corona apps used worldwide is as follows: An app for tracing contacts **must not use any location-based APIs, nor a Bluetooth functionality** and **must not collect any device information that could identify the precise location of users.** This is the regulation in Apple's guidelines.[12] In other words, all governments had to design their corona warning apps in line with the guidelines of market-leading operating systems. Countries which, out of good conviction, adopted their own approach, such as Australia and the UK, could not overcome the technical barriers of the gatekeepers Google and Apple.

Privacy Paradox Even in Times of Pandemic

While Google and Apple use location data for their own commercial services without restriction, exploit it for any purpose and users silently acknowledge this, the Corona-Warn-App shows how the *privacy paradox* is a recurring theme. Democratically legitimated bodies have been and continue to be prohibited from using location data and central data storage for a clearly defined purpose with all rule-of-law guarantees.

A study conducted last year by US telecommunication company Cisco, involving more than 2,600 adults worldwide, revealed that around one third of respondents are "active in data protection". This includes users who take measures such as changing service provider owing to company data policies. Interestingly, this group is prepared to compromise, for example when disclosing their purchase history in exchange for personalised products and services as well as transferring information from smart home loudspeakers in exchange for health and security warnings for the whole family.[13]

A Reminder for the Next Pandemic

No analyses are possible that could lead to more effective political reactions to COVID-19.

There are essentially two types of approaches for virus contact tracing: decentralised and centralised.[14] **From an epidemiological perspective, it is vital to know where contacts or infections take place.** In this crisis, this is often unknown. Information about whether someone met an infected person in the supermarket or in the bookshop has an added epidemiological value[15] that data protection supervisory authorities in Germany cannot seem to comprehend. Recording who becomes infected and at which locations would facilitate analyses that could lead to more effective and equitable policy responses to COVID-19.

No insights that are needed by public and health academic experts.

The first, decentralised approach, like that pursued by Apple and Google, and declared in Germany as the only one that correctly complies with data protection, gives users complete control of "their" data. Our Corona-Warn-App sends an alarm automatically, without a third party having to intervene. To what extent contact persons observe risk reports and how an infection affects whether people transfer data voluntarily is now well-known. **The German**

model safeguards privacy. But crucially, it does not provide any insights that public and academic health experts need to better manage or contain the virus.

The second, central approach takes data from people's phones and stores it in a central system. In Germany, this task could be assumed by the Robert Koch-Institut (RKI), which experts trust to use data in the best possible way. **The central model presents findings necessary for the public health sector to better understand and manage the virus, and to take proactive measures on time**. If an infected user reports their symptoms, they also pass on all their anonymous contacts to the health authority, including some details about the type of contact (such as duration and proximity). On the basis of risk models, the health authority can use the information provided to decide which contacts are most at risk and inform them so that they can take the necessary action. The health authorities can track how the virus spreads. Despite this models' superiority in tracking the spread of the virus and its efficient contact tracing, it could not be implemented either in Australia or the UK due to restrictions imposed by Google and Apple.

The Role of the Digital Gatekeepers Google and Apple

The centralised version, which was tested on the Isle of Wight for instance, worked well when it came to assessing the distance between two users, but was not as good at identifying Apple iPhones. According to a statement by the UK Health Minister Matt Hancock, it might have been more successful if Apple had not limited the use of Bluetooth by third party apps:[16] Regulations underpinning market-leading platforms prevent third-party apps from running in the background and sending Bluetooth signals. This means you have to keep a contact tracing app open in the foreground at all times to ensure it functions correctly. The operating systems of Apple and Google allow software such as the UK's NHS tracing app and the Australian COVIDSafe app to run in a special mode, but only to a limited extent. The apps are a huge drain on the battery life of a device. This results in people not using the app because they want to save electricity.

Summary

No democratic country in the world can point to tangible positive effects from using tracing apps in the fight against corona. However, it is important to note that comparisons are doomed to failure due to different conditions: a rigorous surveillance of quarantine measures (Taiwan), data protection culture and infrastructure (South Korea)[17] or the scale of the pandemic (Australia).

Reasons why apps have failed in democratic countries across the world.

There are essentially two reasons why the apps have failed in democratic countries across the world: data protection and the role of digital gatekeepers (Google (Android) and Apple (iOS)).

Data Protection: Success stories of contact tracing, such as in South Korea, were only made possible through interventions in data protection; such interventions involved serious encroachments[18] that would have been out of the question in a constitutional state. Sensitive personal data was pooled from several sources, and case numbers with motion profiles were visible on a website for everyone to see – horrifying surveillance methods with an enormous potential for danger.

A different question is how data protection practice (not the legal framework) can contribute towards economic and social progress, strengthening the consolidation of national economies within the European Single Market as well as the well-being of citizens. One thing is clear: the stance taken by the data protection authorities in this pandemic was not necessar-

ily cohesive. A fundamental social change of thinking on sharing personal data – especially in national crises – for the public good is unlikely to take place in Germany in a near future. Having said that, the existing legal framework offers much greater leeway for containing the pandemic with innovative means. The scope for political action continues to be unexploited, as the social pressure owing to aggressive misinterpretation of the GDPR is simply too great.

Social rethinking to share personal data for the common good.

In Germany, there is neither a social nor political willingness, let alone the desire, to call assumptions on data protection legislation into question. This is despite massive restrictions on freedom and economic burdens that the current shutdown entails. Almost every attempt to represent data innovation as added value meets with scepticism. Any push during the corona debate towards better use of selected data is often promptly met with horror in public discourse. The tone is mostly loud and shaped by negative connotations. Here, it is worth recalling the debate on the use of common video conference tools in the educational sector.

Along with reforming data protection supervision to make it more coherent, Germany also needs a socially functioning compromise between personal data on the one hand, and innovations and public interest on the other. If this is unsuccessful, misunderstandings and resistance will persist. New tools such as data intermediaries (Data Trusts) may help with this approach, provided they are not stymied by regulatory requirements. We need to hold a data policy debate increasingly from the perspective of the social and economic potential of data.

***Gatekeepers*:** Effective contact tracing is only possible with the integration of market-leading platforms. They set rules and determine principles on how the corona app has to function.[19] The UK and Australia had bitter experiences when their apps failed to comply with rules laid down by Google and Apple. The UK could not ensure the technical functionality of its app, and, in a drastic change of course, switched to a decentralised model based on technology provided by Apple and Google. Despite a number of updates, the Australian app still only functions to a limited extent.

Article 6 of the draft *Digital Market Act* may already offer a remedy for this dependency, with its regulation of the installation and effective use of software applications by third parties, for example. An even more targeted, regulatory solution is also possible within the framework of the announced *Data Act* before the end of this year. The *Data Act* aims to lay down more specific rules for promoting data exchange between companies and between companies and governments. Experiences with the corona apps must be taken into account here.

Outlook

Data has become synonymous with a whole host of ideas and fears, not least due to some comments made in the debate on data protection during the corona pandemic. Along with the reform of data protection supervision to make it more coherent, Germany also needs a socially functioning compromise between personal data on the one hand and innovations and public interest on the other. If this is unsuccessful, misunderstandings and resistance will persist. We need to hold a data policy debate increasingly from the perspective of the social and economic potential of data. And we need new institutions such as the Open Data Institute based on the British model. An Open Data Institute would enrich and drive this discourse.

Even more so, the European Union needs to enable itself to become more independent of the gatekeepers. This can only succeed if digital markets in Europe become contestable. This is not the reality today. The increasing economic clout and technological dominance of large, non-European online platforms not only prevent European business models and innovative

The EU cannot afford to be dependent on the gatekeepers.

power from taking root, but also thwart attempts to act independently, especially during times of crisis. The goal must be that we, as the European Union, can act according to our own values and interests in the digital space as well; without being subject to constraints imposed by a few companies. The clear rules of conduct and standards set out in the Digital Market Act (DMA), should restore a level playing field in future. The swift adoption of the DMA is in Europe's interests. New tools, too, such as data intermediaries, may help with this approach, provided they are not stymied by regulatory requirements. They are probably the most important tool in the framework of the European Data Governance Act, which is also currently pending before the legislators.

1 (EU) Regulation 2016/679 (General Data Protection Regulation), Recital 4

2 Markus Söder on Anne Will on 29 November 2020, https://daserste.ndr.de/annewill/Soeder-Datenschutz,video-import33016.html, similarly Boris Palmer https://www.bz-berlin.de/deutschland/tuebingen-buergermeister-palmer-geht-auf-corona-warn-app-los, as well as Kristina Schröder https://www.zdf.de/politik/maybrit-illner/keine-impfung-keine-lockerung-planlos-in-den-fruehling-sendung-am-4-februar-2021-100.html last accessed on 15 March 2021;

3 Dietmar Neuerer (2021), Woran die Wirksamkeit der Corona-Warn-App leidet, , in: Handelsblatt, 5 February 2021, https://www.handelsblatt.com/politik/deutschland/pandemiebekaempfung-woran-die-wirksamkeit-der-corona-warn-app-leidet/26887560.html?share=twitter, last accessed on 15 March 2021

4 Regulation (EU) 2016/679 (General Data Protection Regulation), Recital 46

5 Ibid.

6 Christine Lambrecht (SPD): "Before there are "far-reaching interventions" in civil rights and liberties, it needs to become clear that these are "absolutely necessary" (ZDF-Morgenmagazin), https://www.zeit.de/politik/deutschland/2020-03/corona-krise-infektionsschutz-gesetz-jens-spahn/seite-2?utm_referrer=https%3A%2F%2Fwww.google.com%2F, last accessed on 15 March 2021

7 *Spiegel Online*, Less Data Protection Does Not Help Fight Covid-19 Either, a guest contribution by Ulrich Kelber https://www.spiegel.de/netzwelt/netzpolitik/corona-warn-app-weniger-datenschutz-hilft-auch-nicht-gegen-covid-19-a-a3a31c6b-e876-44cb-bb84-baf95681b53f, last accessed on 15 March 2021

8 *Tagesspiegel*, https://www.tagesspiegel.de/politik/mit-handydaten-gegen-das-coronavirus-zugriff-auf-bewegungs-daten-mehr-als-problematisch/25615368.html last accessed on 15 March 2021

9 Draft of a law for protecting the population in an epidemic situation at the national level of 20/03/2020

10 Ibid. § 5 IfSG-E

11 Cf. Ulrich Kelber / *Spiegel Online*, https://www.spiegel.de/netzwelt/netzpolitik/corona-warn-app-weniger-datenschutz-hilft-auch-nicht-gegen-covid-19-a-a3a31c6b-e876-44cb-bb84-baf95681b53f, last accessed on 15 March 2021

12 Exposure Notification APIs Addendum https://developer.apple.com/contact/request/download/Exposure_Notification_Addendum.pdf, last accessed on 15 March 2021

13 Cisco Cybersecurity Series 2019, Consumer Privacy Survey. The growing imperative of getting data privacy right, online: https://www.cisco.com/c/dam/global/en_uk/products/collateral/security/cybersecurity-series-2019-cps.pdf (last accessed on 15 March 2021).

14 Ian Levy (2020), The security behind the NHS contact tracing app, in: National Cyber Security Centre, 4 May 2020, online: https://www.ncsc.gov.uk/blog-post/security-behind-nhs-contact-tracing-app (last accessed on 15 March 2021).

15 Cf. Serina Chang, Emma Pierson, Pang Wei Koh, Jaline Gerardin, Beth Redbird, David Grusky & Jure Leskovec, Mobility network models of COVID-19 explain inequities and inform reopening: "Our model predicts that a small minority of 'superspreader' points of interest account for a large majority of the infections, and that restricting the maximum occupancy at each point of interest is more effective than uniformly reducing mobility". https://www.nature.com/articles/s41586-020-2923-3 last accessed on 15 March 2021.

16 Dan Sabbagh and Alex Hern (2020), UK abandons contact-tracing app for Apple and Google model, in: *The Guardian*, 18 June 2020, online: https://www.theguardian.com/world/2020/jun/18/uk-poised-to-abandon-coronavirus-app-in-favour-of-apple-and-google-models (last accessed on 15 March 2021).

17 Nemo Kim (2020), More scary than coronavirus: South Korea's health alerts expose private lives, in: *The Guardian*, 6 March 2020, online: https://www.theguardian.com/world/2020/mar/06/more-scary-than-coronavirus-south-koreas-health-alerts-expose-private-lives; Rory Cellan-Jones (2020), Tech Tent: Can we learn about coronavirus-tracing from South Korea?, in: BBC News, 15 May 2020, online: https://www.bbc.com/news/technology-52681464 (both last accessed on 15 March 2021).

18 Ibid.

19 Cf. Apple addendum: "IF YOU DO NOT OR CANNOT ACCEPT THIS EXPOSURE NOTIFICATION APIS ADDENDUM, YOU ARE NOT PERMITTED TO USE THE APPLE SOFTWARE OR SERVICES"

Imprint

The Author

Pencho Kuzev is Policy Advisor at the Konrad-Adenauer-Stiftung in Berlin. He holds a PhD in Antitrust, Regulatory and European law. Prior to joining the Foundation, he worked for the Deutsche Telekom AG in Bonn in the field of Governmental Affairs and Competition Policy, as well as in attorneys' offices in Hamburg. As a Member of the Department Economy and Innovation at the Konrad-Adenauer-Stiftung, his particular focus is on data economy and the competitive framework in the European Digital Single Market.

Konrad-Adenauer-Stiftung e. V.

Dr. Pencho Kuzev
Policy Advisor
Analysis and Consulting
T +49 30 / 26 996-3247
pencho.kuzev@kas.de

Postal address: Konrad-Adenauer-Stiftung, 10907 Berlin

Publisher: Konrad-Adenauer-Stiftung e. V. 2021, Berlin
Design: yellow too, Pasiek Horntrich GbR
Typesetting: Janine Höhle, Konrad-Adenauer-Stiftung e. V.

Produced with financial support from the German Federal Government.

ISBN 978-3-95721-951-0