THE CORONA APP, A GLOBAL EXPERIMENT IN CONTACT TRACING: HOW ARE THE FUNDAMENTAL RIGHTS OF CITIZENS GUARANTEED? A DUTCH PERSPECTIVE.

Robert van den Hoven van Genderen

Prof. Dr. Robert van den Hoven van Genderen is professor AI & Robot Law at the University of Lapland,
Director of the Center for Law & Internet Vrije Universiteit Amsterdam and founding partner of SwitchLegal Advocaten.
rob.vandenhovenvangenderen@switchlegal.nl

Keywords: ***"Asking people to choose between privacy and health is, in fact, the very root of the problem. Because this is a false choice. We can and should enjoy both privacy and health." Harari, Y.N., The World after Corona Virus, Financial Times, March 22, 2020.***

Summary: *This article discusses the (emergency) measures introduced or activated by governments as a result of the Covid-19 pandemic, and which (un)lawfully restrict the fundamental freedoms of citizens to combat further spread of the virus. In this context, the focus is on the consequences of the introduction of tracking and contact identification, on the "corona-notification application", legitimized as a "scaling tool", and on the recommendations, guidelines and legislation surrounding the use of this corona app.*

1. Introduction

As an expert by experience – I was the first corona patient in Noord-Holland and after 14 days of quarantine I was declared cured – I am constantly amazed and am still amazed at the inconsistency of the measures taken by the various authorities; and also at the behavior of the citizens. Due to the pandemic spread of the corona or Covid-19 virus, almost every state in the world has taken steps to contain the spread of the virus and mitigate its effects.[1] As a result of these measures, national and international travel has come to a standstill, economic traffic has slowed considerably and social contact between people has been reduced to a minimum during the first wave of infections and the resurgence of the virus. Although the measures, implementation and enforcement of the rules differ in Europe (and in the world), the basic principles of the measures are very similar. In the Netherlands, the measures taken and the legal basis thereof arose much debate in society and politics.

1.1. The Measures

Restrictive measures are understandable and necessary in this context, but at the same time limit the freedom to exercise the fundamental rights of the citizens of Europe and other countries. As a result of the containment measures, democratic societies implement rules that are customary in totalitarian states, sometimes without a clear and acceptable legal basis in existing laws. As Wim Voermans (Leiden University) stated in the Dutch national newpaper NRC: "Of course the need is great. But in a constitutional state, necessity does not break a law (certainly not a Constitution)".[2] In addition, these newly enacted rules often involve criminal punishment such as fines or even imprisonment. Due to the unexpected and unpredictable course of the spread of the virus, the development and application of these drastic and society-disrupting measures are not always well

[1] https://www.ecdc.europa.eu/en/geographical-distribution-2019-ncov-cases.

[2] Quality Dutch newspaper [https://www.nrc.nl/nieuws/2020/09/01/coronawet-zet-alle-democratische-principes-op-hun-kop-a4010476].

prepared and substantiated. One of those drastic measures is the introduction of a "tracking & tracing contact application" (Corona App, in the Netherlands: "the Corona Detector") in which the individual citizen is monitored in order to avoid contact with another person infected with covid-19 and be warned. Various authorities have indicated that this application entails risks for the exercise of fundamental rights. It is therefore important to take a critical look at the social and legal impact and the actual usefulness of these measures from a legal and societal perspective, which, incidentally, vary almost daily in terms of elaboration and application. This is inherent to the dangerous space taken up by the government in the emergency measures, which would be legitimized by the unpredictability in the spread and the effects of the virus. An important perspective is that in all circumstances, whenrestricting fundamental rights, one must take into account the positive standards for the protection of such rights. Therefore, one should consider the existing human rights treaties, the European Convention on Human Rights and the General Data Protection Regulation (GDPR). Fundamental rights and freedoms cannot simply be disregarded as is shown in case law based on treaties, European and national legislation.. Governments can only limit these (non-absolute) rights such as freedom of movement, freedom of association, protection of family life, freedom of expression, freedom of information gathering and right to privacy, if there is a legitimate interest, when it is strictly necessary, proportional and as minimal as possible and in particular limited to the necessary period.[3] This article refers in particular to the right to privacy and data protection related to the use of the corona app; and also addresses the disruption of economic and social life that are a result of the (emergency) regulations created to limit the spread of the covid-19 virus, .

2. Range of Measures Taken – The story so Far.

To prevent the spread of the virus, worldwide restrictive measures have been issued, which vary according to whether the spread of the virus becomes more or less severe. The measures taken so far by virtually all governments consist mainly of:

a. Lockdown, i.e. prohibiting freedom of movement, closing (cultural) events, sports facilities, shops, etc.; The lockdown varies in severity, in the Netherlands there was a so-called intelligent lockdown (polder variant);
b. Social distance, i.e. defining a distance (1-2 meters) that people must keep from one another;
c. Prohibition of gathering (more than a specified number of persons); and therefore, de facto prohibition of all cultural and social manifestations, to relaxed prohibitions in times of milder risk of contamination;
d. Closure and/or limitation of educational facilities (part of lockdown) that restrict the right to education; in milder times, limitation of physical education or other restrictions;
e. Media control for corona information, censorship.
f. Prohibition of religious gatherings and closure of religious sites, as a result of which the freedom of (thought, conscience and) religion is limited;
g. Introduction of voluntary or mandatory apps that record personal health and/or apps that record proximity between people to warn people of potential corona risk, i.e. people who will get the virus in the short term.

Violations of these measures are punishable and can even lead to imprisonment and inclusion in a criminal record.[4]

[3] Referring to recital 52 GDPR: Derogating from the prohibition on processing special categories of personal data should also be allowed when provided for in Union or Member State law and subject to suitable safeguards, so as to protect personal data and other fundamental rights, where it is in the public interest to do so, in particular processing personal data in the field of employment law, social protection law including pensions and for health security, monitoring and alert purposes, the prevention or control of communicable diseases and other serious threats to health.

[4] For a global overview see the KPMG report: https://home.kpmg/xx/en/home/insights/2020/04/government-response-global-landscape.html. After it became known that the Minister of Justice and Security himself had violated the rules, a national discussion took place about the height of the fines and the inclusion of the offender in the national criminal record database .

As mentioned, this article mainly examines the effects of the introduction of measures that limit the privacy of citizens, infringe their personal sphere and erase their freedom of movement. The measures restricting freedom of movement and tracking systems using apps are most relevant to this article. In particular, applying these apps in conjunction with public and private cameras and data analysis systems that use advanced algorithms (AI) can be easily misused by governments (or third parties) if not tightly regulated by existing and perhaps new privacy and security rules. The use of big (sensitive) data by third parties, such as the police, employers and tech companies producedby the app, could lead to serious breaches of everyone's privacy if not specifically controlled by, for example, the Data Protection Authority and democratic institutions. It is therefore relevant that the regulations are clear in describing who gets access to the often sensitive data, for what specific purposes, how the data is processed, what security measures are in place, how and for how long the data is used and what guarantees are granted that data is not used for other purposes.[5] Incidentally, the effects of the restrictive regulations extend beyond the invasion of privacy and freedom of movement, and have far-reaching repercussions in the social, cultural and economic fields. The European Commission has already indicated at an early stage (March 2020) that this must be anticipated.

3. Technological Creation and Implementation of the Corona App

To explain the use of the contact app, one relies on the explanation of how the app works by Google and Apple, which after all have created the technological basis for the development of almost all imported and to be imported contact "corona apps".[6] The "corona app" uses bluetooth communication to set up a contact tracing network that collects data about phones that have been in close proximity. Contact tracking is presented as one of the most promising solutions to fight the corona virus, and involves identifying who an infected person has contacted with to try to prevent further infection. The development parties argue that this bluetooth connection would not track people's physical location. It would basically pick up the signals from nearby phones at five minute intervals and store the connections between them in a database. If a person tests positive for the corona virus, he can tell the app that he is infected, and other people can be notified whose phone has passed within close range in the past few days. Public health authorities will have access to this data. Users diagnosed with corona are expected to report it. The system will then warn people if they were in close contact with an infected person. Google and Apple indicate that they have taken sufficient measures to prevent people from being identified, whereby the app sends out anonymous keys instead of a static identity. These keys are renewed every fifteen minutes to maintain privacy. In Europe, a research group called Pan European Preserving Proximity Tracing is working on a pan-European bluetooth proximity tracking app similar to tracking apps in China, South Korea, Singapore and India; although additional account must be taken of privacy requirements.[7] The group indicates that

"The underlying technology, which is being developed in constant exchange with data protection experts and ethicists, should make an important contribution to enabling close cross-border tracing with respect for privacy. It is scalable and open and can be used by any country."

The World Health Organization is also convinced of the usefulness of the corona app and even states that developing and using an app is an international obligation:

"Member States are obliged under the International Health Regulations to develop public health surveillance systems that capture critical data for their COVID-19 response, while ensuring that such systems are trans-

5 See R. 54 GDPR: Such processing of data concerning health for reasons of public interest should not result in personal data being processed for other purposes by third parties such as employers or insurance and banking companies.

6 Brandom&Robertson, the Verge [https://www.theverge.com/2020/4/10/21216484/google-apple-coronavirus-contract-tracing-bluetooth-location-tracking-data-app].

7 https://www.pepp-pt.org/content.

parent, responsive to the concerns of communities, and do not impose unnecessary burdens, for example infringements on privacy".[8]

Despite the positive presentation of the expected results of the use of the app by governments and, of course, by the producers, the positive effects are questionable. Experience in Iceland, the most "app-dense" country, with covid-app was not a game-changer.[9] Even pseudonymized, data collected with the right algorithm can be analyzed, making individuals identifiable. In addition, it has already been found that some apps also contain ad-generating algorithms.[10] In addition, the reliability of the app is questionable*:*

"None of the data sources […] are accurate enough to identify close contact with sufficient reliability".[11]

The choice of the platform and the underlying technology also raised doubts, which was emphasized by the representative of Bits of Freedom, Rejo Zenger, in a meeting organized by the Netherland Association for Media & Communicaton Law (VMC).[12] The Ministry of Health, Welfare and Sport (VWS), for example, has opted for the framework of Apple and Google, which uses bluetooth technology. This while the effectiveness of the use of bluetooth technology for contact research is being questioned. Proximity to a restaurant or any other location, shielded by (plexi) glass will also lead to a report. The same goes for next door neighbours, as well as outdoor activities that seem to pose little risk. In addition to the fact that the introduction of the app cannot lead to the desired result due to incorrect reports, it can also lead to a false sense of security or otherwise have the result that people go into unnecessary quarantine with disruption of work processes or the development of unnecessary psychological problems, such as stress. Minister De Jonge (Health) also indicated, prior to the introduction of the app, that it had not to be considered the "haarlemmerolie" (historical Dutch panacea).

3.1. The Process of Implementing the App

The justification for the Track & Trace App is that lock-down and other restrictive measures to contain the virus can be relaxed because, in combination with further research, more information becomes available about possible contamination by people in their environment.[13] Various countries are therefore planning to use the App as a necessary condition to return to a (new) normal functioning of society and to initiate economic and social activities.

When using the app, it should be kept in mind that all over the world there is a variety of devices and forms of government, ranging from democratically governed countries to more totalitarian states. The purpose of the app should be to prevent contamination by the covid-19 virus. However, there are many more "useful" purposes. This is stated by Patrick Howell, et al, in their Covid Tracing Tracker (CTT) record of every major automated attempt to trace contacts around the world. There was no single standard approach for developers and policymakers. Citizens of different countries saw radically different levels of surveillance and transparency.[14] There is no global standard, but a broad spectrum of technologies and applications. There has also

---

8 Ethical Considerations to Guide the Use of Digital Proximity Tracking Technologies for COVID-19 Contact Tracing Interim Guidance, 28 May 2020, Referring to the International Health Regulations – 2nd ed. Geneva; World Health Organization.

9 [https://www.technologyreview.com/2020/05/11/1001541/iceland-ranking-c19-covid-contact-tracing/].

10 We found code relating to Google's advertising and tracking platforms in 17 contact tracing apps. This includes AdSense, Google's advertising network that allows publishers to make money by showing ads to their users, and also the much more powerful Google Ad Manager, formerly known as DoubleClick for Publishers, which allows publishers to show ads from a huge array of sources. [https://www.top10vpn.com/research/investigations/covid-19-digital-rights-tracker/].

11 Jay Stanley and Jennifer Stisa Granick, The Limits of Location Tracking in an Epidemic, ACLU, April 2020 [https://www.aclu.org/report/aclu-white-paper-limits-location-tracking-epidemic.

12 Lotte Pol, 27 June 2020 "Corona apps – How to (Not) Make One", Mediaforum 2020-4, p. 130.

13 Brandom&Robertson, the Verge [https://www.theverge.com/2020/4/10/21216484/google-apple-coronavirus-contract-tracing-bluetooth-location-tracking-data-app].

14 Patrick Howell O'Neill ,Tate Ryan-Mosley, Bobbie Johnson, May 7, 2020, MIT Technology, A flood of coronavirus apps are tracking us. Now it's time to keep track of them.

been a dangerous development in the implementation and use of the personal data by various authorities. Access to that data can range from medical authorities, to access by tax authorities and police (as is the case of Turkey).[15] The authors of the CTT therefore want to answer the following questions when using the app:

1. Is it voluntary? In some cases apps are opt-in, but in other places many, or all, citizens are forced to download and use them.
2. Are there any restrictions on the use of the data? Data can sometimes be used for purposes other than public health, such as law enforcement – and that can take longer than covid-19.
3. Will data be destroyed over time? The data the apps collect shouldn't last forever. The data should be automatically deleted within a reasonable time (usually within approximately 30 days). Also, app users should be able to manually delete their own data.
4. Is data collection kept to a minimum? Does the app only collect the information it needs to do what it says?
5. Is the application and operation of the app transparent? This last requirement in particular poses problems of interpretation. The problem with the concept of transparency is that it is not unambiguous. Transparency can mean clarity, public availability of the design, an open-source code base, the publicly transparent operation of the algorithm, information for the data subject, the public use of the data, the output and the policy pursued by the government.[16] The set of guidelines drawn up by WP 29 (EDPB) does not provide sufficient clarity in the explanation of the scope of the provisions on transparency. However, once the deployment of the app is activated, there are a number of requirements that must be guaranteed in order for the app to be acceptable for use in a democratic society. In line with these questions and uncertainties, a set of requirements has been combined at the end of this article, based on different sources.

3.2. Introduction of the Apps, a Brief History; Some General Concerns

The Netherlands also seemed unable to avoid the introduction of a corona app. On April 7, 2020, Minister De Jonge indicated the introduction of even two different corona apps, the previously explained "tracking and tracing app" and a so-called health check app to keep in touch with municipal health services and doctors.[17] Several (negative) reactions to the announcement followed almost immediately, including a letter from Catherine Muller (ALLAI) and Natali Helberger (UvA) of 13 April 2020, signed by many, outlining measures to avoid the many risks.[18] It later turned out that it took another six months before an acceptable app could be presented, that would meet technical, security and privacy requirements; and that had an acceptable legal basis. A problematic point of the deployment of these apps and similar proposals is that it is widely accepted that 60% of the population must have downloaded and used the app before its deployment is to be effective.[19] This has caused a lot of criticism for fears that the government would make it mandatory to achieve this coverage. For example, an unofficial survey by Erasmus University in the Netherlands stated that the majority of a group of 900 people would install such an app (only) if it was completely secure and their privacy was guaranteed.[20] In a so-called app-athon, developers of the corona app were asked by the Dutch government in

15 Idem, https://www.technologyreview.com/2020/05/07/1000961/launching-mittr-covid-tracing-tracker/?itm_source=parsely-api.

16 Recital 39 stipulates, amongst other things, that data subjects should be "made aware of the risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing". Recital 60 also refers to the requirement that the data subject be informed of the existence of the processing operation and its purposes in the context of the principles of fair and transparent processing. For all of these reasons, WP29's position is that, wherever possible, data controllers should, in accordance with the principle of fairness, provide the information to data subjects well in advance of the stipulated time limits.

17 https://www.youtube.com/watch?v=74upTyZiMD8.

18 https://www.engineersonline.nl/download/Brief-Minister-President-Rutte-Ministers-De-Jonge-Van-Rijn-Grapperhaus-de-heer-Sijbesma-inzake-COVID-19-tracking-en-tracing-en-gezondheidsapps.pdf.

19 At the moment, 12 November, in Germany 12 mln.downloads, Netherlands 4 mln, resp. 8% and 22%.

20 Netherlands National News Broadcasting, NOS, 1 May 2020 [https://nos.nl/artikel/2332235-meerderheid-zou-veilige-corona-app-installeren.html.

April 2020 to within a very short time create a secure app to be able to track, trace and register. The result of this unrealistic proposal was, of course, a complete failure due to the inability to reach sufficient security and privacy guarantees.

In Germany, the government introduced an app based on "decentralized software architecture" where data would be stored on users' phones, instead of centralized data storage.

It must be taken into account that technology as such is rarely a sufficient solution to a particular problem. For example, the health risks on a psychological level are easily underestimated. The fear of being watched and monitored can have a negative effect on the sense of security and the general health of citizens. This is all the more true when there is no transparency in the process of analysis and use of the (sensitive) data collected by these tracking systems. The sense of security plummets even further as the apps analyze the state of personal health and send it to health authorities for an overview of the situation and for possible identification of new activities and containment rules (or relaxation of those rules).

On the other hand, it can also create a false sense of security because one feels safer by being warned if one has been in the vicinity of an infected person for some time. The choice for the actual implementation of apps must therefore be scrutinized at various points with regard to security and privacy aspects. Apps should be based on privacy by design and transparency requirements as stated in the GDPR.

The question is whether this is sufficient to protect the rights of citizens on a structural basis. Quite a few inaccuracies were found in a worldwide research into 80 imported corona contact apps based on the Google / Apple model that was conducted earlier this year.[21] In deciding whether or not using an app to combat the spread of the virus that will be mandatory for all citizens, all competing interests of those involved authorities, service providers and the public interest – should be considered.[22] There must be openness and transparency during the selection process under the supervision of a parliamentary committee and the privacy regulator. Even after the Privacy Impact Assessment (PIA) was carried out, it appeared that guarantees could not be given. In addition to privacy issues, it is also relevant to monitor the psychological and sociological aspects of the possible implementation of the app. That means it is imperative that the development of the app is not (only) left to a private tech company.

3.3 Intellectual Property Rights and Support for Use

Another relevant aspect that should not be overlooked is the issue of intellectual property rights. If an app is used whereby the government obtains the intellectual property rights, it must be ensured that these rights do not (fully) accrue to the developer who could also use this app for other purposes and would like to offer it for sale to the market. In addition, care must also be taken that if the rights accrue to the government, the use of these rights is only transferred to the government for a limited period of time and for clearly defined objectives. It must also be agreed with the development team that after the usage period for the defined purpose, the app will not be commercially exploited by third parties within the government, such as justice and security services. In addition, the decision-making process for the possible development and use of the apps must be supported by a team of experts from different disciplines who look at both the technical operation and

[21] 25 apps (53%) do not disclose how long they will store users' data for; 28 apps (60%) have no publicly stated anonymity measures; 24 apps (51%) contain Google and Facebook tracking; 9 apps contain Google AdSense trackers; 11 apps contain Google conversion tracking and re-marketing code; 7 apps include code from Facebook. [https://www.top10vpn.com/research/investigations/covid-19-digital-rights-tracker/].

[22] Mittelstadt et. al. have listed a number of factors to be taken into account, including: the presence of an overriding public interest in disease prevention; the likelihood of believing that the use of a person's data will contribute to disease prevention; the risks that those involved may run; understanding the purposes of data use by data subjects; using only the smallest amount of necessary personal data; the inclusion of harm reduction strategies throughout the process. For more information: Mittelstadt B, Benzler J, Engelmann L, Prainsack B, Vayena E. "Is there a duty to participate in digital epidemiology?". Life Sci Soc policy. 2018; 14 (1): 9. Published May 9, 2018. Doi: 10.1186 / s40504-018-0074-1.

the social, psychological and possible economic effects, including behavioral scientists such as sociologists and psychologists, computer scientists, data scientists, epidemiologists, pulmonologists, privacy and data protection lawyers, human rights experts, intellectual property rights experts, administrative law experts, communication scientists and ethicists.

4. The GDPR and the App

Pursuant to Article 5 GDPR, the fundamental principles of the processing of personal data are:

"The processing of personal data must be lawful, fair and transparent, relevant, limited to its purpose, accurate and secure".

It is important that the controller – in the case of the introduction and use of the corona app: the government – must adhere to these principles and as such be held liable in the event of a violation. Recital 4 of the preamble to the GDPR states:

"The processing of personal data must be designed to serve humanity."

This recital is in line with the ongoing debate that modern technology should improve the lives, privacy and security of individuals and not undermine fundamental rights. One of the more difficult requirements to be met under the GDPR is the requirement that personal data must be processed transparently. Article 6 of the GDPR describes the options available to process personal data without the express consent of the data subject. Under E and F, however, this article offers a number of possibilities by mentioning grounds for processing without the consent of the data subject, namely in the vital interest of the data subject or the public interest. Paragraph 3 provides that the processing of the data without consent is governed by: (a) Union law; or (b) the national law to which the controller is subject. However, in several countries it is not clear on which legal basis the restriction of restrictions on fundamental rights rests. Some states have formally declared a state of emergency. This is usually a temporary measure for the duration of the emergency. The democratic content of the Member States though, is not always at the same level.

An exceptional situation can be invoked in the context of the protection of public health. In that case, the fundamental protection, for example as defined in the GDPR, no longer applies in its entirety. This is stated in Article 23 GDPR. The invocation of the exceptional situation must, as stated above, be regulated by law without affecting the essence of fundamental rights. If this state of emergency provision is not applied, there are well-founded doubts about the legality of the restrictive measures taken by the government. Mandatory imposition of the use of a corona app is then unlawful. This is confirmed in the text of Article 22 GDPR that appears to cover the application of the app:

1. The data subject has the right not to be subject to a decision based solely on automated processing, including profiling, which has legal effects on him or her or comparable significant effects on him or her,

but

2. Paragraph 1 shall not apply if the decision: (a) is necessary for the conclusion or performance of a contract between the data subject and a controller; (b) is permitted by Union or Member State law to which the controller is subject and which also contains appropriate measures to protect the rights and freedoms and legitimate interests of the data subject; or explicit consent of the data subject.

Even if the measure is based on the second paragraph of this provision, it will still be necessary for the government to protect the legitimate interests, in this context the fundamental rights, of the data subjects. The transparency requirements for the benefit of the data subject, as indicated in Chapter III of the GDPR, seem difficult to achieve when the app works. In any case, such processing should also be subject to appropriate safeguards, including information specific to the data subject and the right to human intervention, in order to express his or her point of view, to obtain an explanation of the decision taken following such procedure and to contest the decision.

Therefore, except in the event that there is a contract between the government and the data subject, which is questionable, there must be consent from the data subject. If not, app use must be based on legislation with measures to protect the fundamental rights of the data subject. However, these requirements could be overruled by circumstances if the situation is so serious that the government has to apply the restrictions of Article 23 in the case of: (e) economic (f) public (national and EU) interests including public health. This means that the situation must be explained by the government on the basis of specific laws, taking into account

"When such a restriction respects the essence of fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society".

That in this case there is a "disaster" or "crisis" is indisputable with reference to worldwide spread of the corona virus. But until when and to what extent does this crisis extend?

While some fundamental rights may be restricted by the government on the basis of Article 23 of the GDPR, the fundamental rights to protect the democratic society remain guaranteed. Fundamental freedoms such as the free movement of persons, free trade, privacy and even freedom of expression can be restricted in these circumstances, but only as a last resort. However, the essence of fundamental rights must not be jeopardized. This means that there must be a balance between the limitations of rights and the legitimate aim of the measures within a democratic society.

For example, if the government keeps tight control over the provision of information by the government to citizens, it may be doubted whether this is always in the public interest, if not properly motivated, transparent and legitimized by parliamentary scrutiny. When the government provides limited information about the course of infections, the number of cured patients and the effects of the disease on the physical and psychological state of citizens, the question is whether this is in the interest of a democratic society. In addition, handing over sensitive data, such as location, movement and perhaps other activities, provides an opportunity for politicians with dictatorial ambitions to evolve towards total control over their citizens' data. Hence, it is important that such restrictions should be regulated "by law".The problem is that the status of the law is not always clear, according to the European Court:

"The Court notes that the word "law" in the phrase "statutory" encompasses not only statute but also unwritten law."[23]

Not only the law in a statute or acts by parliament is included in the word "law", but also a law in a substantive sense, policy rules and unwritten law. However, the principle is that even with secondary substantive law, citizens have access to the law and should therefore be able to reasonably expect the consequences and sanctions resulting of their actions. In addition, there is a best efforts obligation for the citizen who asks for an opinion from the Court and who must be aware of the meaning of the law. In this sense, a law must be sufficiently clear and precise.[24] The question is whether the previously invoked statutory emergency measures met this criterion, which is discussed in section 4.

Due to national differences in rules and their implementation, a state is given a degree of discretion (margin of discretion). The objective is to observe a fair balance between the interests of the parties involved. A reasonable and fair balance must be struck between the interests involved. The court assesses a state's positive obligation on the basis of this fair balance.

[23] ECtHR April 26, 1979, 6538/74, para. 47 (Sunday Times / United Kingdom).
[24] Idem.

4.1. The EDPB Covid 19 Guidelines, the ePrivacy Guideline

The European Data Protection Board (EDPB) has drawn up guidelines specifically targeting personal data, location data and the use of contact tracing tools, whereby the guidelines seek to protect personal data and privacy as much as possible. It is remarkable that the EDPB starts by mentioning the flexible way in which the GDPR should be interpreted, leaving sufficient room for national authorities.

The EDPB underlines that the data protection legal framework is designed to be flexible and as such can provide an efficient response in mitigating the pandemic as well as protecting fundamental human rights and freedoms. She does, however, warn against overconfidence in the technology:

While data and technology can be important tools, they have intrinsic limitations and can merely leverage the effectiveness of other public health measures.[25]

Here, the EDPB touches on the weaknesses and risks of the introduction and use of the corona app. The introduction of an app is not a panacea. A clear, comprehensive strategy and accompanying implementation policy must be developed, legitimized by legislation before an app can be deployed.[26]

Interestingly, the EDPB's approach to a lawful introduction of the corona app pays particular attention to the application of the ePrivacy Directive. For example, the EDPB states that location data collected from providers of electronic communications should only be processed within the scope of Articles 6 and 9 of the ePrivacy Directive.[27] This means that location data can only be passed on to authorities or other third parties, with the prior consent of the users, anonymised by theprovideror, for data indicating the geographic position of a user's terminal equipment, if it is not traffic data, Also, the storage of data on the user's smartphone and obtaining access to the information already stored is only permitted if (i) the user has given permission or (ii) the storage and/or access is strictly necessary for the information service that is explicitly requested by the user, according to article 5.3 of the Directive. There is a clear preference for the use of anonymised data instead of pseudonymized data. The latter category would still fall within the protection regime of the GDPR. If the so-called proportionality test – a necessary, appropriate and proportionate measure within a democratic society for certain objectives – is passed, then the EDPB only considers the exception of Article 15 of the "e-Privacy" Directive jo. 23 GDPR paragraph 1 as a legitimate ground for processing personal data, in this context storage of location data.[28]

5. National Emergency Ordinances

The so-called emergency regulations in various countries used to restrict and regulate fundamental freedoms still need to be clear and understandable, the European Court of Human Rights said in the Sunday Times judgment. In the Netherlands, the basis for the measures was initially found in the Public Health Act (PHA/Wpg), which regulates the necessary activities to prevent and combat an infectious disease. In the prevention and control of infectious diseases, this act regulates the powers with regard to dealing with an infectious disease crisis. The PHA divides infectious diseases into categories: A, B1, B2 and C. This classification is based on the extent to which mandatory measures can be imposed to protect the population. Category A, the most serious category, includes the corona virus (article 1 under e PHA). The Minister of Medical Care and Sport is

[25] Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak, Adopted on April 21, 2020, p.3 [https://edpb.europa.eu/sites/edpb /files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf.

[26] The efficiency of the contribution of contact tracing applications to the management of the pandemic depends on many factors (e.g. percentage of people who would need to install it; definition of a "contact" in terms of closeness and duration). Moreover, such applications need to be part of a comprehensive public health strategy to fight the pandemic, including, inter alia, testing and subsequent manual contact tracing for the purpose of doubt removal.

[27] 2002/58 / EC (the "ePrivacy Directive") (still!).

[28] For the interpretation of Article 15 of the "ePrivacy Directive", see also CJEU judgment of 29 January 2008 in case C-275/06, Productores de Música de España (Promusicae) v. Telefónica de España SA.

in charge of managing control. The National Institute for Public Health and the Environment (RIVM) advises the Minister on the measures to be taken. The Communal Health Service (GGD) has the task of checking and implementing the measures taken. However, the regulatory authority to take further action rests with the chairman of the security region (a mayor of a larger city in 24 regions) who is responsible for controlling an epidemic of an infectious disease belonging to group A, or an immediate threat thereof. The chairman is therefore exclusively authorized to apply quarantine and other measures by emergency ordinances. With regard to the track and trace app, Article 4 provides the option of processing personal data with regard to the provision of systematic information by the Board of Mayor and Aldermen to the Minister about the implementation of this law. With this provision in hand, the Minister can make personal data disclosure mandatory. This would also apply to the data as a result of a corona app. Geranne Lautenbach indicated during the VMC study day on June 27 2020 that, because the data would be shared with doctors and health insurers, the processing basis for these sensitive medical data should be a medical treatment agreement with the user. This would have the unacceptable consequences for the app that the data would have to be kept for 20 years.[29] If no emergency has been declared by law to activate the rule on extraordinary civil powers, the president of the security regions may not deviate from the basic safeguards in the constitution. Under the Municipalities Act, which also applies to the Safety Regions with regard to this article, this emergency regulation cannot deviate from the Constitution and must be adopted in good time. It must be clear and transparent how measures are applied to citizens. The emergency regulation may therefore in principle not conflict with the articles of fundamental rights of the Constitution. The resulting discourse on the temporal nature of the application of this system of "emergency measures" and the necessity to limit intervention in fundamental rights and to provide them with a democratically controlled guarantee, led to a law (proposal) in a formal sense. The Council of State was also of the opinion that the measures were justifiable due to the life-threatening initial phase of the corona virus. But the legal tenability of the emergency regulations diminishes as the situation lasts. A temporary emergency (statuory)law therefore had to be introduced quickly, replacing the emergency measures.

5.1. The New Dutch Emergency Act

On July 13, 2020, the bill of Temporary Measures Act COVID-19 was sent to the House of Representatives (2e Kamer).[30] To prevent ambiguities, the law is provided with an explanation of 152 pages. It is a proposal with quite a few risks, even with extensive explanation. Below I analyze some of the risks related to the introduction of the app as well as other dangers we face in this bill. The "law" (temporary law) is included in a temporary new chapter Va of the Public Health Act (Wpg) that regulates, among other things, the control of infectious diseases and thus offers the most logical place. The law is considered necessary, because the existing emergency ordinances (also based on the Wpg) by their nature (temporary emergency) should not last too long and are considered to be contrary to constitutional rights.[31]

Where the restrictions affect the fundamental rights in the new law, proportionality and necessity must be clear (Article 58b, second paragraph). In a statutory sense, this law would therefore have the democratic content necessary for radical measures to combat the virus. The new chapter purports to give substance to the requirements of the Constitution and human rights treaties for such restrictions, including the constitutional requirement that a specific basis for the restriction of fundamental rights must be provided in a statutory law. It must also provide scope for determining necessary action and the proportionality of possible measures.

[29] Referring to the provisions of Article 9 paragraph 2 sub h of the General Data Protection Regulation and Article 30 paragraph 3 sub a of the General Data Protection Regulation Implementation Act and 15 Article 454 paragraph 3 of the Medical Treatment Contracts Act.

[30] Act to limit the consequences of the epidemic of covid-19 for the longer term (Temporary Act on Measures covid-19), TK 2019-2020, No. 35 526.

[31] Information about the Constitutional Aspects of (Planned) Crisis Measures, 25 May 2020 (W04.20.0139 / I / Vo), § 11; Parliamentary Documents II 2019/20, 25295, no.234 (Motion).

Although it is argued that the law is not intended to give more powers to the Minister, but has the purpose to protect fundamental rights and to provide for the transfer of powers from the security regions to the municipalities, it is doubtful that no power is slipping back to the regions and the Minister. On closer inspection, it appears that those powers are fairly easily returned to the Minister and the security regions. In addition, there is a risk that the diversity of measures will be increased, causing confusion with panic and unrest as a result. In addition, there is a risk that mayors may take far-reaching measures that constitute an unacceptable interference with fundamental rights, such as imposing curfews, checks behind the front doors, restriction of freedom of assembly, closure of public and private places, etc. Meanwhile (end September 2020), the proposal is accompanied by many amendments in which the interesting combination of the Reformed Protestant Party (SGP) and Green Left (Groen Links) in particular have played a large part, supported by the majority of the other parties, which has significantly improved democratic control.

5.2 Temporary Validity, Introduction of the App?

Interestingly, the law is considered temporary and lapses when it is no longer needed. So, if there is a vaccine for COVID-19, in theory, that's the end of the law. However, this transience is relative. In principle, the validity is expected for six months (Article VIII) or earlier or later. This moment will be presented to parliament. But Chapter Va also applies to the imminent threat of an epidemic (Article 58b, first paragraph) and does this also include the real chance of renewed outbreaks with, for example, a possible modification of the virus?

An amendment has been tabled to the proposed Article that emphasizes the proportionality of the application of the measures to be taken in order to limit the scope for the Minister: public health is inescapable and, compared to other measures, represents the least disadvantage for the person concerned "instead of" insofar as such application is necessary for the purpose referred to in the first paragraph and proportionate to that purpose".[32]

The extension is also reduced to one month. Both extensions require parliamentary approval. The question can be raised whether the use of an app can also be required for a longer time. The elaboration of measures is ratifiedinby ministerial regulation, because the necessary upscaling and scaling down of measures must allow rapid and variable action. Democratic safeguarding would be confirmed by opting for controlled delegation via a preliminary procedure (of 1 week!), whereby the draft ministerial regulation and the order in council would be communicated to both chambers(Senate and House of Representatives) in advance (Articles 58c, second paragraph, and 58f, sub 2). This democratic guarantee can also be set aside if immediate measures are needed to prevent the spread of the virus and to extend the validity of regulations. In addition, the Minister must submit a substantiated statement to the House every month of the measures that apply on the basis of Chapter Va (Article 58t, first paragraph), unless there is no time for this ... Hence, an amendment to Article 58c has also been rightly submitted to ministerial regulations and procedural regulations to be replaced by measures of general administration (AMVBs).[33] The question is whether this change is sufficient to monitor emergency measures.

5.2.1. Article 58s: Safety net, Room for Mandatory Corona App?

This paragraph in the temporary chapter is interesting and dangerouse, because here the Minister is given the opportunity to take further measures in a ministerial regulation, not hindered by the safety precautions designed in the previous provisions. If the Minister does so, he must, within 2 weeks, if possible (!), after pu-

[32] As well as a new Article 2a. The exercise of a power which has been granted will not be exercised if its exercise results in a disproportionate disadvantage compared to the positive effect on public health to be achieved by the measure. House of Representatives, session year 2020-2021, 35 526, no. 21.

[33] TK. 2020–2021, 35 526, nr. 17.

blication in the Government Gazette submit a bill to the House of Representatives . This, therefore, offers the Minister ample opportunities to take unspecified measures in all kinds of areas to combat a corona outbreak; including for example the introduction of a corona app; and even making a corona app mandatory, although this option met with resistance from the Council of State and the Privacy Authority and, until now was laid aside by government. In addition, drafting generally binding regulations, also in the field of (personal) data provision, may be assigned to the chairman of the security regions and to the mayors.. This could concern personal data, such as the temperature measurements of persons, location data whether or not combined with integrated camera images. It is not inconceivable that this data is combined with the results of the app. In a further amendment, it is therefore recommended that this article be dropped because it places too much power on the Minister and puts Parliament out of the game.[34]

5.2.2. Article 58t: Accountability and Provision of Information5

This provision concerns two sides of the spectrum of accountability and information provision. On the one hand, the obligation of the Minister is regulated, whereby account is given for the measures taken and the House is further informed (monthly) about the state of affairs (Paragraph 1). This also includes the mayor's obligation to inform the municipality about the measures taken (Section 4). On the other hand, this provision regulates the obligation of mayors to provide all information that the Minister requires on the basis of this law (free of charge), as well as the manner in which that information is collected (Paragraphs 2 and 3). The latter provision appears to be a license for the Minister to take drastic measures in the field of technological coercive measures for the monitoring and analysis of personal population data in the event of an epidemic flaring up. An amendment has also been tabled to these provisions whereby the chairman of the security region must also be "democratically" accountable for the measures taken to the relevant municipal councils. Also, with regard to other provisions such as the extension of the operation of the "temporary" law, amendments have been submitted so that:

"This bill gives far-reaching powers to the government, without requiring parliamentary approval. The petitioner is of the opinion that extreme restraint is necessary when restricting fundamental rights. It is therefore proposed to reduce the extension to a maximum of one month."[35]

In short, the "emergency law" contains quite a few escape clauses for the Minister to circumvent democratic control, which could include extensive use of the citizen's personal data, perhaps even through the mandatory introduction of the corona track & trace app. Although there is a promise from the Minister that (so far) the corona app will be voluntary, this promise is not carved in stone. The fact that this app was developed by / in collaboration with Google and Apple does not seem to be a problem. After all, it is well known that those companies are known as noble protectors of their customers' privacy. Apple and Google will release a software update on Google Play with a default feature enabled to use the proximity and tracking tool ... [36] Although the Minister initially indicated that no specific legislation was required for the introduction of the law, after the criticism of the Privacy Authority and the Council of State, it was nevertheless decided to include more specific provisions.

---

[34] The petitioners see the importance for the government in times of pandemic to be able to act quickly. The safety net provision in article 58s, however, gives the Minister too much freedom to put Parliament out of play and to take far-reaching decisions independently. The petitioners therefore consider such an article disproportionate. The bill offers sufficient possibilities for setting rules. House of Representatives, session year 2020-2021, 35 526, no. 15.

[35] House of R, session year 2020-2021, 35 526, no. 18 [43] In Article VIII, in the third paragraph, "three months" is replaced by "one month". Lower House, session year 2020-2021, 35 526, no. 19.

[36] Due to the unprecedented worldwide emergency, Play is expediting reviews to enable official apps intended to respond to the COVID-19 pandemic to publish on the Google Play Store. Google takes this responsibility very seriously, and in the interest of public safety, information integrity and privacy, only specific COVID-19 apps that meet the requirements below will be allowed on the Google Play Store. [https://support.google.com/googleplay/android-developer/answer/9889712?hl=en].

6. The Notification App: a Separate Law in the Netherlands

In September 2020, an experiment was started with a notification app based on the platform developed by Apple and Google. According to the Ministry, there is no way to pass on personal data to Apple or Google.[37] This point prompted the Privacy Authority to request a further agreement with Apple and Google in which this would be guaranteed. To my knowledge this has not happened. There are still strong doubts about the transfer of data to these tech giants:

"The telemetry data is encrypted and thus sent completely uncontrollable by the user to servers of various tech giants"[38]

The further legal basis for the introduction of the app has been made possible by including a specific amendment in the Public Health Act (Wpg).[39] The Explanatory Memorandum accompanying the proposal states that the "notification app" is primarily intended to support large-scale source and contact tracing by the GGD.[40] Interesting is the provision in Paragraph 6, which states that the obligation to use the app cannot be imposed on others. It is prohibited to oblige anyone to use the notification application or any other digital means that can be used to identify persons potentially infected with the SARS-CoV-2 virus.

It is at least strange that it is not stated who can impose that obligation and which "others" it concerns. Is it the municipal health services from Paragraph 2? or the Minister from Paragraph 3?[41] The Explanatory Memorandum (EM) to the proposal seems to indicate that this prohibition / obligation applies to and by everyone.[42] Does this also apply to the government? The EM is not exactly crystal clear here. In a statement of the functioning of the app in the EM accompanying the proposal, it is again clearly explained that there are no privacy risks associated with the platform used by Google and Apple.The notification app uses a so-called application programming interface (API) that has been made available by Google and Apple on Android and iOS smartphones respectively, so that the notification app works properly on these operating systems. This API ensures that smartphones on which the app is installed create a so-called Temporary Exposure Key (TEK) every day. These are completely random (cryptographically random), unpredictable and non-reducible numbers. The question is whether this refers to the previously stated criticism that the telemetry data is shared with Apple and Google.

5. Conclusion

The Dutch Data Protection Authority (AP) finds, after further advice of 6 August 2020, that the privacy surrounding the Corona Melder corona app is still insufficiently guaranteed. The Privacy Authority believes that the Minister should make agreements with Google and Apple about the software they provide for the use of the app, that a law should be introduced to properly regulate the use of the app. The AP advises the govern-

---

37 [https://coronamelder.nl/nl/statements/5-privacy/].

38 "The information that Google or Apple receives from the app, via parts of the operating system that cannot be turned off." Fred Hage, Computable, August 27, 2020. [https://www.computable.nl/artikel/opinie/digital-innovation/7044719/1509029/ap-keurt-corona-app-terecht-niet-goed.html].

39 Temporary provisions related to the use of a notification application in the fight against the epidemic of covid-19 and safeguards to prevent its abuse (Temporary notification application covid-19 Act) [https://www.coronamelder.nl/].

40 Article 6d 1. To support the source and contact tracing referred to in Article 6, first paragraph, under c, to combat the epidemic of Covid-19 caused by the virus SARS-CoV-2, a notification application can be used to gain an early insight into a possible infection with that virus. Insofar as necessary, the municipal health services can process personal data when applying this notification application, including personal data about health as referred to in Article 9 of the General Data Protection Regulation.

41 2. Our Minister is responsible for the design and management of the notification application. 3. Our Minister is the controller within the meaning of Article 4 of the General Data Protection Regulation for the processing of personal data with the notification application.

42 The government considers it very important that the use of such a notification app is voluntary at all times. People should never be forced, directly or indirectly, by anyone to use a notification app or other digital means intended to identify people infected with the virus.

ment not to use the app until the recommendations have been followed.[43] The question is whether all these recommendations have been followed. The EDPB states that even if there is location data that is assumed to be anonymous (i.e. actually pseudonymised), it does not in fact have to be anonymous.

Mobility traces of individuals are inherently highly correlated and unique, and therefore, under certain circumstances, may be vulnerable to re-identification attempts by third parties (or government agencies). There are also serious doubts about the usefulness of the tracking and location applications. A well-functioning test and contact follow-up system will in all probability yield a more reliable result without the uncertainties and risks of the complicated implementation of a "corona notification app". The parliamentary debate about the emergency law and the Melding App seems to slightly boost the democratic content of the measure. Let us hope for a serious and critical follow-up of the implementation and enforcement of the measures deriving from the law and the end of the restrictive policy and scaling down of the restriction of fundamental rights of the citizen in the (hopefully soon) disappearance of the Covid-19 virus.

6. Recommended Further Requirements for the Use of a "Corona App"

a. The deployment of the app and the use of sensitive personal data and location data must be based on formal – that is to say by Parliament approved and checked – legal instruments. Any deployment of the apps must be temporary (and therefore reversible), strictly necessary, proportional, transparent and verifiable.
b. The influence of the app on the (social) systems and behavioral patterns requires an underlying support infrastructure (health authority, test labs, psychological and social support, etc.).
c. Effectiveness and reliability of the Track & Trace App is essential because inefficiency and unreliability can lead to a greater risk of contamination. False positives (and negatives) create "false security".
d. All kinds of negative, social chilling effects must be taken into account and measures taken to prevent them as much as possible.
e. There must be a clear, transparent and understandable information policy to inform the population about the purpose and use of the app, and the personal data being processed, and by which parties.
f. Any discrimination or bias in the deployment and use of the app must be ruled out.
g. It is essential that there is parliamentary control over the legal basis and the use of the app.
h. The national privacy authority must have a supervisory function over the use of the app.
i. All information resulting from the use of the app must be destroyed or anonymised when the defined goal is reached. The data made available by the app may not be used by third parties outside the democratically accepted objectives, neither within the government, nor by directly and indirectly involved (commercial) actors.
j. Finally, all "emergency legislation" that legitimizes the use of the app must be immediately put out of action as soon as there is no longer a "disaster" or "crisis", which is clarified in Article 1 of the Wvg. It is indisputable that the rapid, worldwide spread of the corona virus can be described as a disaster and/or crisis, which is not only of local significance, but should not be a reason for any authority to take control of the citizens "for assurance" of protection against (health) crises in the future to take an advance on more permanent extension of powers and long-term use of the app.

[43] The AP has assessed the intended processing on the basis of the documentation and advises against starting the intended processing until the measures referred to in the advice have been. In order to legally carry out the processing within the framework of the GDPR, the AP indicates that the following measures are necessary: 1. Agreements must be made with Google and Apple regarding the Google Apple Exposure Notification framework; 2. It is not possible to use the notification app without a legal basis; 3. The backend server must comply with AVG standards. Advice on prior consultation COVID19 notification app, AP, 6 August 2020 [https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/advies_voorafgebied_raadpleging_coronamelder-app.pdf].