COVID-19 Tracing Apps as a Legal Problem: An Investigation of the Norwegian ‘Smittestopp’ App

Mona Naomi Lintvedt
Doctoral Research Fellow, Norwegian Research Center for Computers and Law (NRCCL), Faculty of Law, University of Oslo
m.n.lintvedt@jus.uio.no

Abstract
In their efforts to curb the COVID-19 pandemic, many countries have introduced contact tracing apps installed on mobile phones with the aim of breaking chains of infection. This raises ethical and legal questions, as these apps have the potential to be used for surveillance of the population. There is pressure to set privacy and data protection aside to allow extensive collection and processing of personal data, while the benefits of the apps remain uncertain. The two versions of the Norwegian COVID-19 tracing app are used as a case study to explore how law and legal norms are made and implemented—or not—in the context of a public emergency. In Norway, the legal question of contact tracing apps has largely been limited to a question of compliance with the GDPR and has excluded a meaningful conversation about the use of apps as pandemic response tools and their impact on rights and freedoms. The normative argument of the article is that to combine a robust form of privacy and data protection with the use of digital tools in a crisis, we need to scrutinize carefully the effects technology choices have on human rights and the rule of law.

Keywords
COVID-19, contact tracing app, GDPR, location data, Smittestopp, privacy

1. Introduction
The first Norwegian COVID-19 contact tracing app ‘Smittestopp’ (hereinafter referred to as ‘Smittestopp 1’) was launched in April 2020. The app was one of the first to be introduced internationally, and also one of the first to be withdrawn; in September 2020, it was officially cancelled by the health authorities, but only after reaching 1.5 million downloads, and attracting criticism from human rights organisations, privacy activists, the Norwegian Data Protection Authority, lawyers, technologists, and the Norwegian Parliament. The core of their critique was the intrusive nature of the app, which in effect could track users’ locations and interactions. Some of the technology choices could be attributed to the problems first movers face in technology development, and the sense of urgency to find effective tools to address novel challenges. However, other aspects of the app’s failure are harder to explain. In December 2020, a new and very different app, also called ‘Smittestopp’ (hereinafter referred to as ‘Smittestopp 2’), was launched. Whereas the first version was criticised for being harmful, the second instalment has been criticised for being both harmless and useless.
The aim of this article is to reflect critically on the application of privacy and data protection legislation in a time of emergency, and untangle some of the legal issues that need to be addressed when opting for intrusive measures. The two versions of the Norwegian COVID-19 contact tracing app (Smittestopp 1 and 2) are used as a case study to explore how legal norms are made and implemented—or not—in the context of a public emergency. The normative argument of the article is that to combine a robust form of privacy and data protection with the use of digital tools in a crisis, we need to scrutinize carefully the effect(s) of technology choices on human rights and the rule of law.

The article proceeds as follows. Section 2 provides an overview of the history of the two contact tracing apps. Sections 3 and 4 discuss the trade-offs between human rights and the obligation of the State to act in a public health crisis. The use of mobile apps enables location tracking of people, and although the intent may be benign, there is an inherent risk of location data being used for surveillance purposes. I argue that this risk must be properly addressed, and the use of contact tracing apps should only be used with a robust legal basis in place. Section 5 gives a critical account of the Data Protection Impact Assessment of Smittestopp 1, and how that assessment failed to serve its purpose. Instead of identifying risks and recommending mitigation measures, the impact assessment justified technical and legal choices that were already made. Thus, it reinforced the intrusive nature of the app, rather than acknowledging and addressing the app’s shortcomings and privacy and data protection risks. Section 6 discusses the differences in having regulation or consent as a legal basis for a contact tracing app. I argue that the app is used to exercise public authority since it is a measure to contain the pandemic. Section 7 describes how the failure of the first app led to data protection by design and anonymisation being prominent in the development of Smittestopp 2, although the law allowed for more functionality in the app. The result is a harmless, but probably useless app. Section 8 contains some concluding remarks to the effect that the use of digital tools in a health emergency is no silver bullet, but requires due considerations of human rights and a robust legal basis.

2. Background: Smittestopp 1 and Smittestopp 2

The Norwegian COVID-19 tracing app, Smittestopp 1 (in English, ‘infection stop’), was launched on 16 April 2020.1 The app was developed by the Norwegian Institute of Public Health (NIPH)2 on assignment from the Ministry of Health and Care Services. It was one of the first COVID-19 tracing apps to be introduced in Europe, following a hurried development phase. The app used Global Positioning System (GPS) and Bluetooth Low Energy (Bluetooth) to register location and proximity data between app users. Personal data was stored centrally for 30 days for contact tracing purposes, and the data would be rendered anonymous before being used for modelling purposes. The combination of location data and centralised storage would enable large-scale surveillance of the population. This

---


2. In Norwegian, ‘Folkehelseinstituttet’ (FHI).
attracted some criticism, but did not deter users from downloading the app. The app quickly reached 1.5 million downloads.³

After a short honeymoon phase, there was a steady decline in the app’s usage. The app had technical problems and drained the battery life of mobile phones, and there was also increasing concern about privacy and data protection and a lack of transparency. This prompted a polarised public debate about the app’s technological shortcomings and privacy-intrusive nature. This culminated in May 2020 with a joint statement from a self-organised group of technology and privacy experts along with other concerned citizens, calling on the NIPH to migrate to a more privacy-friendly solution.⁴ Furthermore, an expert group appointed by the Ministry of Health and Care Services to examine the source code of the app recommended changes to improve data protection and security,⁵ the Parliament demanded changes in the app,⁶ Amnesty International classified the app as a highly invasive surveillance tool,⁷ and the Norwegian Data Protection Authority opened a formal investigation.⁸ In July 2020, the Data Protection Authority issued a temporary ban on processing of personal data collected by the app.⁹ The NIPH decided to discard the app and delete the personal data.¹⁰ The Ministry of Health and Care Services commissioned work in October 2020 on a new app, which was launched on 21 December 2020. The new app is also named Smittestopp (and, for the purposes of this article, is called ‘Smittestopp 2’), and re-uses code from the Danish app Smittestop.¹¹ Smittestopp 2 is based on the protocol for exposure notification by Apple and Google (GAEN), using Bluetooth and storing information locally on each mobile device.¹² The development process was open, with the NIPH inviting external experts and activists to participate in reference groups.¹³ The Data Protection Authority has described the new app as more privacy friendly, although this does not mean that it has given the app its formal approval.¹⁴ As of 23 October 2021, the app had been downloaded just over 1 million times.¹⁵

³ Out of a population of 5.4 million, although the number of downloads is higher than the number of people that used the app since the app could be downloaded several times.
⁴ ‘Joint statement on contact tracing for Norway’ (Medium, 19 May 2020) <https://medium.com/@jointstatementnorway>. Initiators of the statement formed an informal group ‘Smittestoppwatch’ on Slack, where I have been a member since September 2020.
⁵ Ministry of Health and Care Services, ‘Endelig rapport for kildekodegjennomgang av løsning for digital smittestoring av koronaviruset’ (18 May 2020) <www.regjeringen.no/contentassets/88ec3360adae44a1a9635fd6c1a58ca/200520_rapport_ekspertgruppa_smittestopp.pdf>.
⁶ Innst 385 L (2019–2020) Vedtak 711 ‘Midlertidige endringer i smittevernnloven (hjemmel for forskrifter om isolering og begrensninger i bevegelsesfrihet mv.)’.
⁸ Datatilsynet, ‘ Starter kontroll av FHIs Smittestopp-app’ (27 April 2020) <www.datatilsynet.no/aktuelt/aktuelle-nyheter-2020/starter-kontroll-av-smittestopp/>.⁹
¹² For information about the GAEN protocol, see eg Apple and Google, ‘Exposure Notifications: Using technology to help public health authorities fight COVID-19’ <www.google.com/covid19/exposurenotifications>.
¹³ NIPH posted regular updates and documents, see ‘Oppdateringer om arbeidet med nye Smittestopp’ <www.fhi.no/om/smittestopp/digital_smittesporing/>.
¹⁴ Datatilsynet, ‘Ny Smittestopp lansert’ (21 December 2020) <www.datatilsynet.no/aktuelt/aktuelle-nyheter-2020/ny-smittestopp-lansert/>. Note at the same time that the Authority does not normally give formal approvals of such tools.
3. Regulatory quality in a time of crisis

To control a communicable disease such as COVID-19, contact tracing is an essential public health tool to break the chains of transmission of the virus. Contact tracing is the process of identifying people who may have been exposed to infection to prevent further transmission. Efficient contact tracing requires adequate human resources, as contact tracing is, at least traditionally, a predominantly manual task.\(^\text{16}\) The COVID-19 pandemic has led to a surge in the development of digital contact tracing apps by public health authorities—or, more accurately, proximity tracing apps\(^\text{17}\)—as potential tools to supplement the manual contact tracing process, or even to control the pandemic.\(^\text{18}\) Traditional contact tracing relies on trust and communication with the population; thus, ethics, privacy, and data protection are essential factors to be taken into account at all stages of contact tracing.\(^\text{19}\) With contact tracing apps capable of collecting and further processing large amounts of data, their potential threat to human rights and privacy is even more prevalent.\(^\text{20}\)

In the ongoing public debate and research on COVID-19 contact tracing apps, some commentators have framed privacy preservation on the one side and fighting the pandemic and saving lives on the other side, as mutually exclusive choices:

> It hardly needs saying that the saving of lives and reduction of suffering are of immense moral importance and there are strong reasons to support efforts to achieve this. The ethical assessment of an innovation capable of making a contribution to addressing these harms needs to be understood and analysed against the dramatic scale of the deaths and suffering represented by these data.\(^\text{21}\)

This juxtaposition fails to see the fundamental role that ethics, human rights, and privacy play even in a health emergency.

Although a human right, the right to privacy is not absolute. Article 8(2) of the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) allows interference by a public authority in the right to respect for private life if the interference is in accordance with the law and necessary for, inter alia, the protection of health. Similarly, the rights to privacy and data protection laid down in Articles 7 and 8 of the Charter of Fundamental Rights of the European Union (CFREU) may be limited if subject to the general principles of legality, necessity, and proportionality.\(^\text{22}\)


\(^{17}\) I use the term ‘contact tracing app’ since this is the popular name that has gained traction, although ‘proximity tracking’ is a more correct term, as pointed out by the WHO: ‘Proximity tracking is often conflated with “contact tracing”, although contact tracing is a broad public health discipline, and proximity tracking is a new technique for aiding contact tracing’. See WHO, ‘Ethical considerations to guide the use of digital proximity tracking technologies for COVID-19 contact tracing: Interim guidance’ (28 May 2020) <www.who.int/publications/i/item/WHO-2019-nCoV-Ethics_Contact_tracing_apps-2020.1>.

\(^{18}\) Luca Ferretti, Chris Wymant, Michelle Kendall, Lele Zhao, Anel Nurtay, Lucie Abeler-Dörner, Michael Parker, David Bonsall, and Christopher Fraser, ‘Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing’ (2020) 368(6491) Science 619 <https://doi.org/10.1126/science.abb6936>.

\(^{19}\) WHO (n 16).

\(^{20}\) WHO (n 17).

\(^{21}\) Michael J Parker, Christopher Fraser, Lucie Abeler-Dörner, and David Bonsall, ‘Ethics of instantaneous contact tracing using mobile phone apps in the control of the COVID-19 pandemic’ (2020) 46 Journal of Medical Ethics 427, 428 <http://dx.doi.org/10.1136/medethics-2020-106314>.

\(^{22}\) cf Article 52 CFREU. Since Norway is a member of the European Economic Area (EEA) but not of the European Union (EU), the Charter is not directly applicable to it. The Charter is therefore not discussed further in this article. However, I recognise that it has a significant indirect impact on Norway through, inter alia, rulings of
The prohibition on processing of special categories of data, including health data, in Article 9 of the EU General Data Protection Regulation (GDPR)\(^2\) does not apply when it is necessary to process data for the purpose of provision of health services and for reasons of public health and protection against serious cross-border threats to public health, including communicable diseases.\(^2\) The extent of processing of personal data for health purposes, including necessary measures in a pandemic, relies on the legal basis provided by national legislation. The legal basis must ensure that the processing will be subject to suitable and specific safeguards so as to protect personal data and other rights and freedoms.\(^2\) Thus, it is health legislation rather than the GDPR that can limit the measures that can be taken in combatting the pandemic.

The European Data Protection Board (EDPB) issued a statement in March 2020 as a reminder that the GDPR is not hindering measures to fight the coronavirus pandemic, but that the measures taken must respect the general principles of law, ensure the protection of personal data, and be proportionate and limited to the emergency period.\(^2\) In April 2020, the European Commission issued guidance on the use of COVID-19 tracing apps in relation to data protection, the advice being not to use location data, since it is not necessary to track the movement of individuals for tracing purposes, and it would also be disproportionate and raise security and privacy issues. In the Commission’s view, proximity data using Bluetooth would be sufficient.\(^2\) The following week, the EDPB adopted guidelines emphasising the use of proximity data instead of location data for tracing apps, and advised that decentralised storage was preferable.\(^2\) Both the Commission and the EDPB recommended that the use of contact tracing apps should be voluntary, with a legal basis in national health legislation to provide legal certainty for the processing of personal data.

The legal basis for Smittestopp 1 was the Regulation on digital infection detection and epidemic control in connection with an outbreak of COVID-19 (hereinafter ‘Smittestopp 1 Regulation’).\(^2\) The Regulation was a delegated act based on the Communicable Diseases Act,\(^2\) and was sanctioned by Royal Decree\(^3\) without prior public consultations. Moreover,
as a delegated act, its drafting did not involve direct parliamentary scrutiny. An explanatory memorandum (‘statsrådsforedrag’) from the Minister of Health and Care Services gave some background to Smittestopp 1, noting that the app’s legal basis was the Regulation, but that use of the app would be voluntary.32

At the time, the Government already had extensive powers to derogate from existing laws and pass legislation without approval of the Parliament or prior public consultations.33 The Regulation entered into force 27 March 2020, and the app was launched on 16 April. This left three weeks that could have allowed for public consultation.34 The hasty legislative procedure and lack of public consultation have been criticised by the Coronavirus Commission,35 which stated that public consultations should always be carried out for emergency measures, if necessary ex post, and particularly when measures are intrusive and based on derogation.36

The explanatory memorandum omitted any reference to the statement of the EDPB, nor was the regulation amended in line with the EU recommendations. Although the recommendations from both the European Commission and the EDPB are not legally binding, contravening them should have prompted a thorough re-assessment of the legislation and the technology of Smittestopp 1. Instead, the project went on as planned, and at the press conference for the app, the then Minister of Health and Care Services gave his assurances that the app was compliant with the GDPR and the guidelines from the EU.37

4. Smittestopp as a legal problem

4.1 How technology choices created legal dilemmas

§ 4 of the Smittestopp 1 Regulation specified that the app would use location data from mobile phones. The assumption was that the use of location data would make it possible to supplement and even replace some of the manual contact tracing.38 The app would use GPS to record the movement and location of the user, and a combination of GPS and Bluetooth to make proximity records between the user and other mobile phones with the app installed. The location and proximity data was uploaded to central storage every 20 minutes. The app stored proximity data for mobiles within ten meters from the user, while the persons being identified as close contacts would be those within a range of two meters. Instead of reducing the amount of data to those of potential close contacts before uploading, this would be

33. Communicable Diseases Act § 7-12.
34. By comparison, in the course of three weeks, the Ministry of Finance and the Tax Administration prepared a new law and a regulation for a temporary grant scheme for businesses, including approval from the EFTA Surveillance Authority, at the same time as developing a technical solution in collaboration with private and public partners. This made it possible to do necessary adjustments in both the legislation and the solution as the project progressed. See Skatteetaten, ‘Fikk på plass omfattende kompensasjonsordning på rekordtid’ <www.skatteetaten.no/en/about-the-tax-administration/jobb-it/kompensasjonsordning/>.
35. The Coronavirus commission was appointed by the King’s Council in April 2020 as an independent commission to review and assess the management of the pandemic by Norwegian authorities. See mandate <www.koronakommisjonen.no/mandate-in-english/>.
38. Explanatory memorandum (n 32).
done by an analytical tool after the data was stored. The location data was stored for 30 days, although only the 14 previous days are relevant for contact tracing. The choice of extended storage time was not specifically commented upon in the explanatory memorandum, but later explained to be necessary for validation purposes.39

Using location data, efforts should have been made to mitigate the privacy and data protection risks and comply with the data minimisation principle laid down in Article 5(1)(c) GDPR. For example, the proximity data could have been stored locally on the phone, and only uploaded or accessed for use in the case of an infected user. Instead, the data of all users was uploaded.

After the app was launched, it emerged that although data was being collected for all users of the app, it would first be piloted in three municipalities. The pilot started on 27 April 2020 and was described as a validation of the app and a test of whether the notification function would work.40 However, the app was rolled out nationally and promoted to the whole population, regardless of residence, as a critical factor to combat the pandemic. Hence, data from users in the other 353 municipalities was collected unnecessarily.

The effect of the use of the combination of GPS and Bluetooth for this purpose was uncertain, with the NIPH describing such data use as ‘new and innovative’.41 Indeed, the app had an air of experimentation. Discussions about the choice of technology and its impact on rights and freedoms were absent in the explanatory memorandum, the ensuing Data Protection Impact Assessment, and in other communications from the NIPH.

4.2 An incomplete articulation of human rights

In the public debate around Smittestopp 1, some argued that location data is already regularly collected and stored by mobile operators and various apps; ‘someone’ already knows our whereabouts at any time.42 This view was also shared in some of the academic scholarship. For example, two scholars wrote:

The question is not whether to use new data sources—such as cell-phones, wearables, video surveillance, social media, internet searches and news, and crowd-sourced symptom self-reports—but how.43

Another group of scholars argued that ‘installing a tracing app that primarily aims at helping in a noble cause of keeping the community safe from spreading the COVID-19 disease […] should not cause undue concern’.44

The right to health is not explicitly protected by the ECHR, but in a complaint about the French State’s handling of the COVID-19 crisis, the European Court of Human Rights (ECtHR) noted that the State still has positive obligations to take necessary measures to

39. NIPH, ‘Data Protection Impact Assessment Smittesporing’ (13 April 2020) 8 <www.fhi.no/contentassets/67d2db7c1ba4e209070c9606b1c7a0/dpia-smittestopp.pdf>.
41. NIPH (n 39) 3.
protect the lives and physical integrity of persons in their jurisdictions, including in the domain of public health.\(^4\) The International Covenant on Economic, Social and Cultural Rights also places the State under an obligation to protect the right to health by taking necessary steps for ‘the prevention, treatment and control of epidemic, endemic, occupational and other diseases’ (Article 12(2)(c)).\(^4\) Public health may be invoked as a ground for limiting certain rights in order to allow the State to take measures dealing with a serious threat to the health of the population or individual members of the population.\(^4\) But even as States limit individual freedoms to address this public health emergency, they must assure that such limitations are reasonable, proportionate, non-discriminatory, and grounded in law.\(^4\)

The question is therefore whether the use of location data for the purpose of contact tracing and monitoring of the spread of the infection would be a necessary and proportionate measure.

Location data can reveal not only a person’s location or mobility, but also other personal traits and preferences based on the places a person frequents.\(^4\) Even if the purpose of Smittestopp 1 was not to surveil or track every movement, the data made it possible to do so.

In *Uzun v Germany*, the ECtHR noted that the use of GPS for surveillance of a bomb suspect was proportionate and necessary because less intrusive methods had proved insufficient, the surveillance was carried out for a short time, and was limited to GPS tracking of a car. In the Court’s view, the measure had the legitimate aims of protecting national security, and the statutory provisions in place provided adequate and effective safeguards against abuse.\(^5\)

By comparison, the use of Smittestopp 1 would allow continuous surveillance of the location and movements of persons carrying mobile phones, their location and proximity to other app users for a period of seven months with the possibility of prolongation, and would be used in addition to other intrusive infection control measures.\(^5\) The legal basis was a Regulation drafted unilaterally by a Ministry.

The explanatory memorandum to the Smittestopp 1 Regulation mentioned briefly that privacy and the requirements of the GDPR should be taken into account, but did not recognise the potential for surveillance by use of the app. Neither Article 8 ECHR nor the respect for the right to private life pursuant to § 102 of the Norwegian Constitution were mentioned. There was no assessment of the necessity and proportionality of the measure or whether this would be a legitimate limitation of the right to private life with the aim to protect public health. The regulation neither fulfilled the requirements of ensuring adequate and effective safeguards nor had the legislative quality expected of a limitation of fundamental rights and freedoms.

---

50. *Uzun v Germany*, no 35623/05, 2 September 2010.
51. Smittestopp 1 Regulation, §§ 2, 4 and 10.
The lack of consideration of human rights and the Constitution is striking (although not limited to Smittestopp, as pointed out by the Coronavirus Commission) and poses a threat to the rule of law. In a crisis, even something seemingly benign as rolling out a tracing app requires due regard to human rights and the rule of law. The cost of ignoring this may lead to long-lasting harms to fundamental rights and freedoms and trust in government.

4.3 The inadequate application of the law

4.3.1 The bundling of purposes

The Smittestopp 1 Regulation stated two purposes for the app: 1) enabling swift tracing of persons who may be infected by COVID-19, and giving advice to persons who may be infected; 2) monitoring the population to surveil the spread of the infection, and evaluating the effect of the infection control measures.

The Regulation clearly stated that the use of the app would be voluntary. The explanatory memorandum explained that consent would not be an appropriate legal basis for the processing activities of the app, as users could feel pressured to use it without a full understanding of the consequences. Although not formally based on consent, the memorandum described the conditions for voluntary use as similar to that of freely given consent.

However, when users downloaded the app, their personal data would be used for both contact tracing and monitoring purposes. The NIPH also introduced a sub-purpose to the second purpose of monitoring, stating in the DPIA that the data could be used additionally for research. The research purpose was not mentioned in the regulation or the explanatory memorandum, nor in the information to the users. Before the app was launched, the Norwegian National Research Ethics Committee advised the NIPH to separate the two purposes, and to ask for consent for the purpose of monitoring, which the Committee considered to be research.

In June 2020, the Parliament adopted a decision that the app should be redesigned with two separate purposes.

The EDPB guidelines stated that large scale monitoring of location and/or contacts in COVID-19 tracing apps could ‘only be legitimised by relying on a voluntary adoption by the users for each of the respective purposes.’ For Smittestopp, the voluntariness only extended to a choice of whether or not to use the app, and did not enable the user to choose voluntarily either of the two purposes. This bundling of purposes further enhanced the privacy-intrusive nature of the app.

---

52. Coronavirus Commission, see English summary chapter 2.2 para 7 <www.regjeringen.no/contentassets/5d388acc92064389b2a4e1a449c5865e/no/sved/01kap02engelsk.pdf>.
55. Smittestopp 1 Regulation, § 1.
56. Smittestopp 1 Regulation, § 2.
57. Explanatory memorandum (n 32).
58. NIPH (n 39) 6–7.
60. See above (n 6).
61. EDPB (n 28) para 24.
4.3.2 The lack of anonymisation

Mathematical modelling and analysis of infectious disease outbreaks play an important role in the public health response to epidemic diseases, and as input to informed policy decisions. Analysing mobile phone data can be used to model changes in mobility and patterns of possible transmission of the COVID-19 virus. In February 2020, Norway began modelling movement patterns utilising data from mobile operators. Collecting data about people’s movements from the Smittestopp app was considered a useful additional source of data.

The Smittestopp 1 Regulation specified that no ‘directly identifiable personal data’ could be processed for the monitoring purpose. The formulation resembled a term in the Norwegian Health Register Act defining ‘indirectly identifiable health data’ as health data where name and similar unique identifiers are removed, but where the data can still be linked to a person. Thus, the data is personal data as defined in Article 4(1) GDPR.

The term was not elaborated upon in the explanatory memorandum, so it is unclear if this was a deliberate formulation to allow the use of personal data or if it was a way of saying the data should be pseudonymised or even anonymised. In their guidelines, the EDPB emphasised that preference should always be given to use anonymised data rather than personal data for modelling purposes. On this point, it seems that the Norwegian regulation went further, and opened the possibility of personal data being used.

However, the understanding of the NIPH was that anonymous data should be used for the monitoring purpose. This was also the information given to the public. For data to be anonymous, there can be no reasonable possibility of re-identifying individuals. Location data is difficult or even impossible to render anonymous since most people have distinct movement patterns, as has been well documented by research. Although the aim was to use only anonymous data for the monitoring purpose, there was a gap between the ambition and the implementation. The system for handling and analysing the data for monitoring was not developed before the app was launched and data collection started. This was partly due to the massive amount of data. Thus, 9 billion GPS positions were collected over three weeks, but not used.

65. NIPH (n 39) 7. See also Birgitte Freiesleben De Blasio, ‘Modellering av covid-19-epidemien i Norge’ in Hans Petter Graver, Øystein Hov and Tonje Tønjum (eds), Tilt i koronaens tid (Dreyers forlag 2020) 53, 69.
66. Smittestopp 1 Regulation, § 4.
67. Lov 20 juni 2014 nr 43 om helseregistre og behandling av helseopplysninger (helseregisterloven) § 2 (f).
68. EDPB (n 28) para 14.
69. NIPH (n 39) 6–7.
70. Recital 26 GDPR.
72. NIPH (n 39) 3, 7; and Ministry of Health and Care Services (n 5) 17, 26, 29.
It is a core principle of data protection law that only necessary data should be processed, and data should be minimised in both quantity and quality in accordance with the purpose.\(^{74}\) With the lack of anonymisation techniques, backend systems and analytical tools to process the location data, the collection of data for monitoring purposes was excessive, a breach of the pledge of anonymity, and non-compliant with the GDPR.

5. Data protection impact assessment: ticking the box

If a planned processing activity might pose a high risk to people’s rights and freedoms, a Data Protection Impact Assessment (DPIA) has to be performed prior to the processing.\(^{75}\) The EDPB considered that a DPIA should be carried out before any COVID-19 tracing apps were implemented.\(^{76}\) Similarly, the explanatory memorandum to the Smittestopp 1 Regulation assumed that a DPIA would be required.\(^{77}\)

The purpose of a DPIA is to ‘describe the processing, assess its necessity and proportionality and help manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data by assessing them and determining the measures to address them’.\(^{78}\) A DPIA requires several steps: 1) the planned processing must be described, including the purposes and the legitimate interest of the controller, 2) the necessity and proportionality of the planned processing in relation to the purposes must be considered, 3) the risks to the rights and freedoms of the data subjects must be considered, and 4) any measures to mitigate the risks must be assessed.\(^{79}\) The DPIA is not limited to assessing the rights of the data subjects as outlined in the provisions of the GDPR. The reference to ‘rights and freedoms’ is wider, and although not spelled out in the GDPR, can be understood as the full catalogue of the European fundamental rights framework, including the ECHR and CFREU.\(^{80}\)

The DPIA for Smittestopp 1 was completed 13 April 2020, only three days before the app was launched.\(^{81}\) Although the DPIA concluded before any processing started, the intention of a DPIA is not met when it is completed too late to influence the technological and organisational measures for the processing activity in a meaningful way, while an early DPIA can contribute to informed decision-making and to the protection of societal concerns.\(^{82}\)

The DPIA for Smittestopp 1 was primarily a description of how the app would work. Some risks were mentioned, but brushed off. Alternatives were not discussed. For example, it was admitted that there were no tools or procedures in place to anonymise personal data for the monitoring purpose.\(^{83}\) Whether anonymisation was feasible was not discussed, but should have been. A possible outcome could have been not to include this feature.

---

74. Article (5)(1)(c) GDPR.
75. Article 35 GDPR.
76. EDPB (n 28) para 39.
77. Explanatory memorandum (n 32).
78. Article 29 Working Party, ‘Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679’ (WP 248rev.01) 4. These guidelines have been endorsed by the EDPB.
79. Article 35(7)(d) and Recital 90 GDPR.
81. NIPH (n 39) 27.
83. NIPH (n 39) 7.
In the DPIA, the only assessment of the risk to rights and freedoms was a mention of the ECHR without reference to specific articles. A short explanation was given: ‘The societal benefits outweigh the right to respect for private life. The use of the app will make it possible to lift other restrictions since the measure is “more targeted”’. This brief assessment failed to consider the risks from the point of view of the affected persons, and was rather an exoneration of the app.

Hence, the DPIA for Smittestopp 1 bore the mark of a pro forma assessment. A proper assessment early in the process could have identified and considered the inherent privacy and data protection risks of using location data on a large scale, influenced the design choices for the app and revealed inadequacies in the regulation.

6. Smittestopp 2: a fragile legal basis
6.1 The European approach: law as legal basis
The European Commission and the EDPB have recommended legislation as the legal basis for the COVID-19 tracing apps, but with voluntary use of the apps. As they aptly note, the voluntary use of an app would not mean that the legal basis for processing would be consent. The most relevant legal basis would be the necessity for the performance of a task in the public interest (Article 6(1)(e) GDPR), or necessity for reasons of public interest in the area of public health or for health care purposes (Articles 9(2)(h) and 9(2)(i) GDPR). The legal basis should be laid down by law, ensuring safeguards and specifying, inter alia, the categories of data that would be processed and the purpose of processing. The Commission emphasised that due to the nature of the personal data involved and the circumstances of the pandemic, relying on law as the legal basis would contribute to legal certainty for the use of apps. In some instances, existing laws regulating the health authorities processing of personal data would be appropriate, while in other cases new legislation would have to be enacted.

The recommendations of the EDPB do not exclude the use of consent as a legal basis, but underline that ‘the controller will have to ensure that the strict requirements for such legal basis to be valid are met’. Hence, consent must be freely given, specific, informed, and unambiguous. The ‘freely given’ criterion restricts use by public authorities since there is an imbalance in power between the parties. As Recital 43 GDPR states, ‘where the controller is a public authority […] it is therefore unlikely that consent was freely given in all the circumstances of that specific situation’. This means that consent can only be used in cases where there is an actual choice for the user and the processing is not an exercise of public authority. Although the use of consent as a legal basis is not entirely excluded for public authorities, the examples given by the EDPB guidelines on consent permitting such use involve authorities’ processing of personal data for rather banal purposes, such as consent to the use of e-mail addresses to receive notifications on road maintenance work from a municipality.

---

84. Ibid 18–19 (author’s translation).
85. EDPB (n 28) paras 29-31.
86. European Commission (n 27) para 3.3.
87. Ibid.
88. EDPB (n 28) para 32.
89. Article 4(11) GDPR.
It can be questioned whether the EDPB guidelines on COVID-19 tracing apps actually took the requirement of balance between the parties sufficiently into consideration when including consent as a possible legal basis for the apps. As mentioned in the guidelines, ‘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’. As long as these apps are part of the pandemic response and both provided and promoted by the health authorities, it is hard to see how there can be a proper balance between the parties and thus freely given consent.

The majority of the EU/EEA Member States have legislation as a legal basis for the personal data processing for the COVID-19 tracing apps, or a combination of consent and legislation. These Member States include Belgium, Croatia, Denmark, Estonia, Finland, France, Iceland, Italy, Latvia, Malta, the Netherlands, Poland, Portugal, and Spain. Countries that have consent as a legal basis include Cyprus, Czechia, Ireland, Germany, and Lithuania.

6.2 The Norwegian approach: replacing regulation with consent

As noted above, the Smittestopp 1 Regulation has been repealed. This occurred on 9 October 2020, following the decision to discontinue Smittestopp 1. A few days prior, the Ministry of Health and Care Services gave the NIPH the task of making a new app based on the GAEN protocol. Although eventually copying the Danish app, the NIPH and the Ministry did
not copy Denmark’s use of legislation as the legal basis for the app. The use of the Danish app is voluntary, but the regulation for the app sets out, inter alia, the purpose and categories of data, the deletion of data, the roles of the involved health authorities, and the interface with other systems and registries.\(^\text{115}\)

For Smittestopp 2, the legal basis is consent. The assignment letter from the Ministry specified that the use of the app should be voluntary and based on consent from the user.\(^\text{116}\) There is no documentation of whether a legal basis in law was considered—for instance by amending the Smittestopp 1 Regulation—or why consent was considered to be the most appropriate legal basis.\(^\text{117}\)

In the DPIA for Smittestopp 2, the NIPH argued that the processing of personal data by the app would not be an exercise of public authority, and thus consent would be an appropriate legal basis for processing in accordance with Articles 6(1)(a) and 9(2)(a) GDPR.\(^\text{118}\) Furthermore, ‘the app is not meant as a contact tracing tool for the health authorities or to be used for analysis of the spread of infections, but as a tool for each user for their own digital contact tracing’.\(^\text{119}\) However, in this brief discussion, the NIPH seems to fail taking into account the fact that the app is promoted as ‘one of several measures to contain the spread of COVID-19’,\(^\text{120}\) and thereby potentially falls within the scope of the legal basis provided by Article 6(1)(e) GDPR—i.e as being both ‘necessary for the performance of a task carried out in the public interest’ and ‘exercise of official authority vested in the controller’.

6.3 Digital contact tracing as exercise of public authority

The government’s roles and tasks must follow directly or indirectly from law in accordance with the rule of law and the legality requirements of the ECHR and § 113 of the Norwegian Constitution. Particularly in a time of emergency, legislation can provide much needed legitimacy and transparency about decisions that will impact the daily lives of citizens. For a public authority, limiting the discussion of the legal basis to what is necessary for compliance with data protection legislation is clearly not sufficient.

When Smittestopp 2 is installed and exchanging tokens with other mobile phones, the NIPH is not part of the processing. However, as the use of the app is one of the measures to contain the pandemic, it cannot be disconnected from the formal authority of the NIPH. If the right to provide a contact tracing app is exclusive to the NIPH, it should also be mandated by law.

Limiting the legal assessment to the app and the data stored on the phone is also a simplification of how the app works. It is not a standalone tool. Smittestopp 2 only works in an ecosystem with other registries and procedures. When a person has a positive test result for COVID-19, the person can voluntarily notify others through the app.\(^\text{121}\) To avoid false

---

116. Ministry of Health and Care Services (n 114).
117. The decision by Parliament (n 6) stated that the user should consent to two separate purposes. However, taking the debate into consideration, it should rather be understood as a requirement to separate the purposes and not as a statement of the proper legal basis.
119. Ibid 15 (author’s translation).
120. NIPH, ‘Om Smittestopp’ (author’s translation) <www.fhi.no/om/smittestopp/om-smittestopp/>.
notifications, the person has to verify their identity with the national identity number\textsuperscript{122} through the ID-portal\textsuperscript{123} and collect a verification token from the Surveillance System for Communicable Diseases (MSIS).\textsuperscript{124} When the verification is received in the app, a notification will be sent to other app users who have been in close contact with that particular phone.

The use of a verification process connecting the app to a central health registration system is only used by Denmark,\textsuperscript{125} Estonia,\textsuperscript{126} and Norway. The first two-listed countries have legislation as a legal basis for this integration. The other European apps do not use a log-in to a health register. Instead, when a person receives a positive test result, the person will be provided with a unique code to activate the app’s notification procedure.\textsuperscript{127} Thus, for most other apps, there is no technical interface between the app and the infrastructure and registries used by the health authorities.

On the other hand, the design of Smittestopp 2 is reliant on the interface with the ID-portal and MSIS, both of which were made for public authority purposes. With this dependency on a national health registry, it would have provided more clarity with legislation in place for the app. In the DPIA for Smittestopp 2, the NIPH refers to the MSIS Regulation, but makes no reflections on the need to regulate the interface between the app and the registry, despite the purpose limitation of the MSIS Regulation.\textsuperscript{128} The Smittestopp 1 Regulation specified the role of the NIPH and the interaction with MSIS. If this was necessary to regulate Smittestopp 1, it can be questioned why it was not also necessary for Smittestopp 2.

6.4 The fiction of consent
Because valid consent must be freely given, specific, informed, and unambiguous,\textsuperscript{129} use of consent as legal basis poses requirements to the promotion of the app. A message from the Prime Minister, similar to the one given in spring 2020, that people should download the app to get their freedom back,\textsuperscript{130} would have disrupted the ‘freely given’ element of consent.

Consent relies on assumptions about human decision-making where the person is in control of their own data by reading and understanding the information given and making an informed and conscious choice. Behavioural research indicates that many people do not understand the information, and simply consent whenever confronted with a consent request, instead of thinking through the consequences of providing or refusing consent.\textsuperscript{131} Even in cases where the information is hard to ignore, studies suggest that no more than

\begin{itemize}
  \item All residents in Norway have a unique identity number registered in the National Population Register (‘Folkeregisteret’).
  \item The ID-portal is managed by the Digitalisation Agency.
  \item MSIS is managed by NIPH: see Forskrift 20. juni 2003 nr. 270 om Meldingssystem for smittsomme sykdommer (MSIS-forskrifter) [Regulation concerning the collection and processing of health data in the Norwegian System for Communicable Diseases and for notification of infectious diseases] (MSIS Regulation) § 1-5.
  \item The users confirm their positive test results from the app by authentication with NemID to validate against test results in the Danish Microbiology Database: see FAQ Smittestop <https://smittestop.dk/en/q-and-a>.
  \item The code is provided by SMS, e-mail, phone or in person: see eg Croatia StopCovid-19 (n 95) paras 6, 8; Latvia ApturaCovidovid (n 102) para 5.2.6.
  \item MSIS Regulation § 1-3.
  \item Article 4(11) GDPR.
  \item Speech by Prime Minister Erna Solberg, ‘Ny app vil stoppe smitte raskere’ (16 April 2020) <www.regjeringen.no/no/aktuelt/ny-app-vil-stoppe-smitte-raskere/id2697812>.
\end{itemize}
50 percent of people will read and understand simple and transparent privacy notices. If the information required for consent is hard to understand for privately provided apps and online services, it is legitimate to ask why it would be easier for an app provided by a public authority.

Consent requires clear and concise information to the user, yet it can also lead to information overload or simplification. The privacy policy for Smittestopp 2 states that the use of the app will ‘make infection tracking faster and easier by allowing the process to take place without any kind of manual processing after you or others have taken the initiative to send a notification’. This is inaccurate, as the app cannot replace or even supplement manual contact tracing. The dependency between the app and other measures needs to be explained, so users do not get a false sense of security when using it.

In the DPIA for Smittestopp 2, one of the considerable risks identified was that consent would not be sufficiently informed since the complexity of the app would make it hard to give easily accessible, clear and sufficient information. The suggested mitigation measure was to give comprehensive and adapted information to the user when installing the app and in the privacy policy. The DPIA did not elaborate whether there was a risk that the information was not adapted to the various language skills and abilities in the population. Furthermore, there was no discussion of the consequences this would have for the validity of consent, and thus the implications for the lawfulness of the processing.

The app and the privacy policy were initially available in Norwegian and English. Since late March 2021, the app has also been available in Arabic, Lithuanian, Polish, Somali, Tigrinja, and Urdu. The information given at the time of consent is a condensed version of the privacy policy in the chosen language, and the user will be directed to the English version for more information. In addition, posters about Smittestopp 2 have been made in 41 languages. However, the posters provide simplified information ending with ‘if you do not understand what is written, ask someone to explain it to you’. This lack of adaptation of language to various skills and abilities in the population may not meet the condition for information given ‘in an intelligible and easily accessible form, using clear and plain language’.

Although the ambition was a high uptake of Smittestopp 2 to ensure the app’s usefulness, it took over three months before it was available to a wider public than Norwegian and English speakers. At the same time, it was known that persons with another country of origin were affected significantly harder by COVID-19 than the rest of the population.

133. NIPH (n 121) (author’s translation).
134. WHO (n 17).
135. NIPH (n 118) 37.
138. Article 7(2) GDPR.
and that there had been lack of information adapted to these groups. If the app turns out to be efficient in early detection of infection, this lack of proper information may lead to adverse effects for minority groups.\footnote{UN Office of the High Commissioner, ‘COVID-19 and minority rights: Overview and promising practices’ (4 June 2020) \url{www.ohchr.org/Documents/Issues/Minorities/OHCHRGuidance_COVID19_MinoritiesRights.pdf}.
}

The use of consent downplays the role of public authority: there is an implication that since consent can be used, there is no imbalance of power and exercise of public authority, which may imply in turn that the app is not intrusive. Relying on consent from users to process their personal data will also limit the influence the public can have in shaping the measures to which they will be subject. In my view, the main concern about the use of consent by a public authority, even for something seemingly inconspicuous as an app, is that it excludes an open public debate. Whether to use an app or not, what purposes the app should have and which data it should process, whether the app should be integrated with other measures, and how long it should be used, are all policy questions. If an app is used as an infection control measure, it should be regulated as such and be possible to scrutinise and control.

### 7. From risk to irrelevance

In developing Smittestopp 2, great emphasis has been put on data protection by design as understood and stipulated by Article 25 GDPR. While this is admirable (and legally required), the principle of data protection by design has been applied to such a strict degree that the app likely ends up having negligible utility.

Preserving the anonymity of close contacts has been a main rule for the development process. This is in contrast to manual contact tracing. According to the Communicable Diseases Act § 5-1, a person with an infectious disease has a duty to contribute to contact tracing by giving up names of close contacts. As long as legislation is in place for the use of contact information for contact tracing, it could be possible to include this functionality in the app. This functionality is present in the Icelandic app, where the user can upload registered contacts to the contact tracing team after verification of a positive test.\footnote{Line Fransson, ‘Har ikke oppdaget coronasmitte’ Dagbladet (16 May 2020) \url{www.dagbladet.no/nyheter/har-ikke-oppdaget-coronasmitte/72454590}.} The distributed form of contact tracing (or contact notification) in Smittestopp 2 is therefore not limited by law, but by the design choices for the app.

Yet, although it would be possible to disclose the information, it may not be advisable to do so out of concern for the legitimacy of Smittestopp 2. Since the cancellation of the first app, the public’s distrust of the app and their attention to privacy has been high. This could make it impossible to launch an app with functionality allowing the use of any personal data.

The speed at which alerts can be sent to contacts relies on the infected person using the app for this purpose. The manual contact tracing may move faster for known contacts since there is a delay in registration of test results in MSIS.\footnote{NIPH (n 118) para 2.2.} With Smittestopp 1, no persons apart from already-tracked contacts were notified.\footnote{Line Fransson, ‘Har ikke oppdaget coronasmitte’ Dagbladet (16 May 2020) \url{www.dagbladet.no/nyheter/har-ikke-oppdaget-coronasmitte/72454590}.} For Smittestopp 2, the current number of people having used the app for notification since 21 December 2020 is 5,664 out of a total of
210,239 registered infected persons in the same period, and the number of people having received notifications is unknown.

With both Smittestopp 1 and Smittestopp 2, it has been emphasised how effectively an app can help in containing the pandemic. Contrary to the strictly mathematical model suggesting that an uptake of 60 percent of the population could contain the infection, other models suggest that the efficiency of apps in identifying infected people might be less than random testing. The experience with the Singaporean app is that human-to-human contact tracing is still more efficient and reliable, and the app performs better with a ‘human-in-the-loop’ system. Thus, care should be taken not to be over-reliant on technology.

The effects of the apps remain to be proven. One of the most comprehensive studies to date concludes that the privacy risk outweighs the benefits since ‘there is not enough evidence to support that such an app would help slow down the running contagion’, but that an app can nonetheless be ‘useful to spread awareness and encourage modifications in people’s behavior’.

8. Concluding remarks

Strict privacy and data protection rules were blamed for the unsuccessful attempt at Smittestopp 1, yet, as discussed, the law allows intrusive measures to be used in times of crisis. However, the legitimate use of privacy-invasive measures requires that any restrictions of the right to private life are reasonable, proportionate, non-discriminatory, and grounded in law. It is insufficient to limit the legal questions to data protection and compliance with the GDPR, as was done for the Norwegian COVID-19 contact tracing apps.

The role of legislation is fundamental in ensuring that the rights and freedoms of people are respected in exceptional circumstances. The legislative process, even in a state of emergency, serves a democratic function in opening for debate and involvement by the public and upholding the rule of law. This is also true for a seemingly minor app.

The Norwegian experience shows that an app is not simply an app. It can threaten human rights if not implemented correctly. Digital tools are not mere tools or digital representations of manual procedures; they bring with them other possibilities and threats which must be taken into consideration.

Moreover, the government’s use of digital tools in a health emergency should be recognised for what it is: the exercise of public authority. The question should not be limited to.


145. Ferretti (n 18).


149. The Minister of Health and Care Services criticised the temporary ban by the Data Protection Authority (see above n 9), and claimed this would limit access to vital data to contain the spread of infection. See eg Frode Andresen and Bjorn Langsem, ‘FHI-fiasko: Tvilte i mai’ Dagbladet (1 October 2020) <www.dagbladet.no/nyheter/fhi-fiasko-tvilte-i-mai/72895330>; Espen Moe Breivik, Benedicte Bratås, and Pernille Solheim, ‘Høie ber nordmenn beholde Smittestopp-appen’ VG (18 June 2020) <www.vg.no/nyheter/i/0n52G6/hoeie-ber-nordmenn-beholde-smittestopp-appen>. 
how such tools should process personal data, but extend also to whether digital tools should be used. This pandemic has shown that digitalisation does not necessarily provide legitimate quick fixes, and may introduce new threats to our rights and freedoms in addition to the health threat.

Before introducing other digital tools in this pandemic or the next, due consideration of human rights must be taken as a first step. Conventions on fundamental human rights allow limitations and even derogations, but proper assessments must be made of the necessity, proportionality, and legality of the planned measures. At the risk of stating the obvious, even such basic steps can be ignored or forgotten in a crisis as this article shows.

The next step is to ensure a robust legal basis in law. Public authorities should not take shortcuts by relying on consent in the belief that it gives people more autonomy. Rather, they should acknowledge that democratic participation is ensured by the legislative process—provided that the legislation is clear and compatible with the rule of law.

Furthermore, the use of digital tools must not be introduced as isolated gadgets, nor should technology more generally ‘lead the way’. The direction should be set by conscious and deliberate choices that take into account human rights, ethical and societal impacts, and the respect for privacy and data protection when designing and using digital tools. In the context of a pandemic or other related challenge, those tools should complement rather than steer public health measures.

There is little evidence so far of the usefulness of contact tracing apps. More research is needed about their effects as tools to curb the pandemic, their impact on human rights and society more generally, as well as their broad ethical and legal implications. Through such research, we might do better next time.

Work on this article was carried out under the aegis of the research project ‘Vulnerability in the Robot Society’ (VIROS), funded by the Norwegian Research Council. Thanks are due to Professor Kristin Bergtora Sandvik for the inspiration and encouragement, as well as to Heather Broomfield and the anonymous reviewer for valuable suggestions and comments.