CMG
• LEGAL
AVOCATS

The French Covid-19 Mobile Application:

Apprentice witchdoctors juggling with privacy rights or just Much Ado About Nothing?

Laura Ngoune
Barrister-at-Law & Avocat
CMG LEGAL – Paris

On June 2, 2020, the French government launched a Mobile App called **"*StopCovid*"**, subsequent to a vote by the Parliament and the Senate in May[1].

Essential features of *StopCovid*

StopCovid is a centralised, Bluetooth based technology that operates on pseudonymised data. It is described as only storing on a centralised server contacts history when two mobile devices are within one meter away for at least 15 minutes.

StopCovid should continuously operate on pseudonymised data to protect the users' identity.

The App does not require users to input personal information such as name, email, age, mobile number etc. After it is downloaded, users are attributed a permanent pseudonym that is linked to the device itself. Subsequently, they are issued new temporary pseudonyms every 15 minutes. The information transmitted to the centralised server is limited the temporary pseudonyms, while the permanent user's pseudonym shall never be communicated to the centralised server.

The legal issues raised by StopCovid

As the government intends to use the App to monitor private citizens interactions in their private life, some fear the App may could be used as a state-wide surveillance tool thus interfering with private citizens right to private life[2].

Considering that the App will collect and store data from users' mobile devices, should such data processing be governed by the EU GDPR and national law on data protection[3]?

StopCovid has been approved by the French Data Protection Authority ("CNIL")

[1] *https://www.lemonde.fr/pixels/article/2020/05/27/l-assemblee-donne-son-feu-vert-pour-stopcovid-l-application-francaise-de-suivi-de-contacts-contre-le-covid-19_6040964_4408996.html*
[2] *Art. 2 of the Declaration of the Rights of Man and of the Citizen of the 26th August 1789*
[3] *GDPR (EU) Regulation 2016/679, French Data Protection Act of 1978 as amended, Art. 8 ECHR*

Prior to the implementation of the App, the French DPA was consulted on two occasions.

Initially, the French DPA stated that the use of a Bluetooth system and pseudonymisation of users' data guarantee some level of privacy. However, the French DPA also considered that since the App will be installed on natural persons' mobile devices and be linked to a centralised server, the App will ultimately process personal data connected those persons, including sensitive data such as health information within the meaning set by the GDPR[4].

Subsequently, the French DPA indicated that the implementation of the App meets **the legality, necessity, and proportionality test**[5]:

- The government elected to process personal data on consent and public health interest[6] basis, therefore meeting the **legality test** *as per* the French DPA's initial opinion.

- The French DPA found that the **necessity test** was met by the government because the App was integrated into a global strategy to fight the virus. The App could be seen as a necessary tool for early identification of infected or exposed persons with a view to facilitating their assistance by health professionals in the nation-wide effort to slow down the spread of the virus.

- The French DPA also considered that the processing of collected data to be **proportional** and **compliant** with privacy law and GDPR on several grounds:
  - There is no legal obligation to download or use the App. The voluntary approach is guaranteed by the fact that there aren't any adverse or positive consequences regardless of the decision to use the App or not;
  - The processing of the data is limited to inform and guide users, raise awareness and improve the effectiveness of contacts tracing through the study of statistical data. The App supposedly collects adequate, relevant, and limited data necessary for the intended purpose;
  - Infected users remain free to upload their infected status on the App, and users notified of their "exposure" to the virus remain free to contact a health professional;
  - The App will only transmit pseudonymised data of users "exposed" to the virus rather than the pseudonyms of users *infected* with the Covid-19, while ensuring that no link is stored between the infected users and the "exposed" users;

[4] CNIL Opinion n°20006919 of 24th April 2020, p.3 and 4: https://www.cnil.fr/sites/default/files/atoms/files/deliberation_du_24_avril_2020_portant_avis_sur_un_projet_dapplication_mobile_stopcovid.pdf
[5] CNIL Opinions n°20006919 of 24th April 2020, n° 2020-051 of 8th May 2020 and 202-056 of 25th May 2020
[6] Art. 6 and 9(2)(i) of the GDPR

- The appointed Data Controller is the Ministry of health ensuring the App is fully implemented in the government strategy to fight the pandemic;
- The collected personal data will be stored for a maximum period of six months after the end of the Health State of Emergency and shall be deleted at such date. Users' proximity history with "exposed" or infected users shall be deleted within fifteen days. The collected data shall not be processed or transferred outside of the EU;
- Users may delete their personal data at any given moment from their mobile phone and the centralised server using a functionality of the App before uninstalling it;
- The App source code will be made available to the public.

The formal vetting by the French DPA did not, however, discard criticisms.

Concerns raised by the legal profession

StopCovid has been received with some scepticisms by members of the legal profession.

The French National Bar Council considers that users' consent when given in a state of panic and fear could not be truly be viewed as free and informed[7]. The President of the National Bar Council pointed out that the use of pseudonymised data may not prevent the risk of such data being stored somewhere[8].

The Paris French Bar considers that the pseudonymisation of data alone does not guarantee anonymity especially in case of data breach or fraudulent use of the collected data. While anonymization is irreversible, pseudonymization on the other hand is reversible. The French DPA pointed out that strict securities measures ought to be put in place in order to prevent re-identification through a study of correlations between the connections identified.

The fallacy of users' consent and the effectiveness of StopCovid

The approval of StopCovid by the French DPA was based on its legal foundations: users' consent and public health.

However, it was revealed on June 17, 2020 that the App collects more data what was announced and what is strictly necessary for the intended purpose. In fact, StopCovid collects and transfers all contacts made by users no matter the time spent in "close vicinity" (in this case less than 10 seconds through a wall!). Therefore, users do not know the **full scope** of the data collected nor the intended ultimate purpose of such data collection, which undermines the principle of consent.

[7] *https://www.gazette-du-palais.fr/wp-content/uploads/2020/05/15.CNB-MO_2020-05-14_LDH_etat-urgence-sanitaire-libertes-fondamentales_FERRY-BOUILLONFinal-P.pdf*
[8] *https://www.affiches-parisiennes.com/stopcovid-tracking-et-respect-des-libertes-fondamentales-10237.html*

CMG
• LEGAL
AVOCATS

The concerns raised by experts and the legal profession regarding the risks of social mapping and government surveillance cannot be ignored in light of this revelation.

Moreover, StopCovid was justified by its potential effectiveness as a preventive measure. According to Oxford University, at least 60% of the population must use a contact tracing app for it to be effective[9]. In France 25% of the population do not own a smartphone[10], therefore cannot download StopCovid.

Only 1,5 million people downloaded the App to-date[11], for a population of 67 million[12], ie approximately 2% of the population[13]… As at the end of June 2020, approximately 500,000 users had uninstalled the App from their mobile device.

Furthermore, by opting to operate on a centralised system, the French government elected a system that prevents interoperability with iOS and Android decentralised Apps launched in other EU States. With the reopening of the borders, StopCovid will not be able to exchange any information with the smartphones of foreigners in France or abroad, therefore failing to meet the "paneuropean" approach advocated by the EU Commission on April, 8, 2020 (Recommendation (UE) N° 2020/518).

A strong warning to the public from experts in cryptology and computer security

In April, 473 experts in cryptology and computer security, signed a letter designed to warn the public against the serious risks of social mapping and mass surveillance by the state through the use of the StopCovid App.

A successful hack of the centralised server entails the hacker getting access to all the data collected, such risk being emphasized by the use of a Bluetooth technology.

Besides, experts doubted the efficiency of contact tracing with a Bluetooth system, pointing out the risk of inaccuracy deriving from the inability of the system to tell if two individuals are actually within 1 meter or more from one another, or close proximity through a wall.

[9] https://www.research.ox.ac.uk/Article/2020-04-16-digital-contact-tracing-can-slow-or-even-stop-coronavirus-transmission-and-ease-us-out-of-lockdown
[10] *https://sante.journaldesfemmes.fr/fiches-maladies/2630463-stop-covid-application-tracing-contact-coronavirus-c-est-quoi-gouvernement-obligatoire-autorise-lancement-sortie-2-juin-disponible-telecharger-combien-fois-cnil-controle-succes/*
[11] https://www.leparisien.fr/societe/stopcovid-1-5-million-de-telechargements-pour-quelques-notifications-11-06-2020-8333706.php
[12] *https://www.lepoint.fr/societe/population-la-france-compte-67-millions-d-habitants-14-01-2020-2357666_23.php*
[13] *https://www.lemonde.fr/pixels/article/2020/06/10/l-application-stopcovid-connait-des-debuts-decevants_6042404_4408996.html*

CMG
• LEGAL
AVOCATS

***Much Ado About Nothing?* Apprentice witchdoctors should not be underestimated**

Civil liberties concerns arise from the use of the App.

They also arise, perhaps more importantly, from a *de facto* acceptance by the public of a generalised digital monitoring of individuals' private life, which could only be mitigated by the marginal number of persons that decided to become active users of the App, provided such decisions were taken with civil liberties concerns mind.

Those concerns are not counter-balanced by the prospect or even the hope of any real impact in the prevention of the spread of virus, nor by any other legitimate purpose. And they will certainly not when, as the day may come, lists of non-users will be made on the ground they pose a potential threat to the general population, or being a user will be imposed by health insurance companies, transport services, employers, … "for your own good".

July 2020