SEEDIG intersessional project on COVID-19 tracking apps in SEE+

Recommendations for governments / public health authorities and developers regarding a human rights-based approach to design and deployment of COVID-19 tracking apps

September 2020

Executive summary

Mobile tracking appeared to be one of the most popular tools used by the governments during the COVID-19 outbreak in an attempt to curb the virus dissemination. While some applications were designed to trace contacts of the infected individuals and subsequently alert people at risk, others primarily focused on monitoring compliance with self-isolation regimes. Many governments in South-Eastern Europe and the neighboring area (SEE+) have either already deployed some versions of COVID-19 mobile tracking apps (e.g. Armenia, Bulgaria, Croatia, Cyprus, Greece, North Macedonia, Russia, Turkey, Ukraine) or are considering their deployment (Romania).

These Recommendations are the end product of the SEEDIG intersessional project on COVID-19 tracking apps that was launched with the aim to sensitise stakeholders (governments, developers, civil society, academia, etc.) about the level and state of deployment of tracking apps in SEE+ region, as well as their human rights implications. Within the scope of the project, a dedicated working group (WG) examined local practices from nine SEE+ countries and two countries from outside the region.[1]

The findings indicate a tendency of governments across the region to resort to the deployment of tracking apps as part of the overall efforts to combat the pandemic. At this point, it is difficult to evaluate the efficiency of the analysed apps as official statistical data is largely unavailable. However, several drawbacks and challenges posed by the application of these apps are already on the surface. These Recommendations provide a short overview of the key human rights concerns raised by large-scale mobile tracking and are addressed to governments/public health authorities and developers for careful consideration when developing policies and/or deploying mobile apps.

[1] Detailed overview of the COVID-19 tracking apps in the region is available in the annex.

1. Background

1.1. Purpose of Recommendations

The Recommendations pursue the following purpose: suggest possible solutions to governments/public health authorities and developers aimed at mitigating negative human rights implications of the tracking apps.

To achieve this purpose the WG conducted an overview of the country-specific practices of using COVID-19 tracking apps in the SEE+ region.

1.2. Overview of country-specific practices of using COVID-19 tracking apps in SEE+

As part of this project the following countries were analysed (that have or are reported as working on some forms of COVID-19 related apps): Armenia, Bulgaria, Croatia, Greece, North Macedonia, Romania, Russian Federation, Turkey, Ukraine. For comparative purposes, the group also looked at Germany and Hungary, although these countries are beyond SEE+.[2] During the assessment phase it was identified that different forms of tracking apps are deployed in ten analysed countries (Armenia, Bulgaria, Croatia, Germany, Greece, Hungary, North Macedonia, Russia, Turkey, Ukraine). Among the mapped countries, Romania does not (yet) have an app. Among other SEE+ countries that have mobile tracking apps but were not specifically analysed within the project are Azerbaijan, Cyprus, Georgia, and Slovenia, as well as Serbia that recently announced its plans to launch an app. However, given the overall similarity of such apps, the provided Recommendations might be equally useful for stakeholders in these countries.

The conducted research revealed that mobile applications were deployed by public authorities either to monitor individuals during the quarantine period (Ukraine, Greece) or to track infected people and to prevent further dissemination of the virus (Armenia, North Macedonia, Germany, Hungary, Russia). Most of the applications presume voluntary use. In all researched countries, the authorities claim that deployed apps comply with data protection laws, however, not all of them provide transparent information to the public regarding data processing policies, data subjects' rights, and applied algorithms.

Although the applications were developed to help monitor virus dissemination and protect individuals from the risk of getting infected, concerns have been raised over issues such as

[2] The WG incorporated these two countries into its research work for the purpose of assessing whether practices in SEE+ region are similar or different from those outside the region, especially considering that the majority of countries in the region are outside the EU. In particular, the WG was interested in comparing whether countries directly bound by the GDPR are in any way more cautious about users' privacy. Moreover, Hungary was chosen due to its proximity to the analysed region, while Germany because its app is often presented in the media as a good practice.

privacy and physical integrity. At the same time, some authorities have acknowledged that the implementation of new technological solutions in response to COVID-19 entails new challenges related to ensuring information security, providing proper safeguards to human rights, complying with the core data protection principles including data minimisation and purpose limitation, which are highly interlinked with the requirement to obtain data subjects' consent before processing personal data, etc.

Functionally, the analysed apps in SEE+ countries vary by purpose and methods of data processing and storage. For classification purposes, analysed apps were clustered into the following groups: a) centralised contact tracing apps (Armenia[3]); b) decentralised contact tracing apps (North Macedonia, Croatia[4]); c) centralised apps used for monitoring self-isolation and validation of movement requests (Ukraine, Russia, Greece[5]); d) apps for symptoms tracking, which may be combined with other tracking functions (Bulgaria, Turkey).

2. Challenges and concerns

Throughout its research work, the working group has identified the following challenges and concerns that have been raised with regard to some or all of the analysed apps.

- Rather rushed approach to launching the apps without proper research of potential human rights implications and without sufficient guarantees that proper safeguards have been put in place.
- Lack of official and/or scientific data as to the effectiveness and efficiency of tracking apps, as well as any measurement mechanisms to assess their impact.
- Failure of governments to properly justify the proportionality and necessity of using the apps.
- Potential negative impact on privacy and freedom of movement.
- Increased risk of discrimination, especially against infected individuals based on their health status and vulnerable social groups (if misused, apps might significantly contribute to profiling and stigmatisation based on collected data).
- Limited trust in governmental apps in the light of concerns related to the ethical and transparent collection and processing of data (including sensitive data such as health information).

[3] Outside of SEE+ Hungary is an example of countries that fall within this group.
[4] Outside of SEE+ Germany is an example of countries that fall within this group.
[5] Currently, the app is not used in Greece due to alleviation of quarantine restrictions.

3. Recommendations

3.1. Governments and public health authorities are recommended to:

- conduct needs and human rights impact assessment prior to making a decision to deploy a tracking app;
- have a clear and detailed deployment strategy before proceeding to the tracking app roll-out, in particular, specify the purpose, scope, timeframe, target users, expected efficiency, etc.;
- collect users' feedback on the app and make any necessary adjustments to improve the deployment strategy and increase the efficiency of the app;
- be mindful of accessibility issues;
- avoid creating any extra administrative burden for individuals (e.g., entrance to public buildings subject to installing an app);
- ensure a fully voluntary use of tracking apps (individuals who do not consent to install an app shall not be treated in a less favorable way or penalised);
- propose alternative, less intrusive options to individuals opting out from using tracking app;
- prioritise apps designed for processing minimal and anonymised personal data;
- apply the highest privacy standards, even beyond the national legislation;
- ensure transparency of data collecting, processing, and retention;
- envisage clear and limited timeframes for processing and storage of collected data;
- elaborate clear and user-friendly privacy and data retention policies;
- limit the categories and number of parties that have access to users' personal data to what is strictly necessary for the declared purpose of the app;
- ensure that any necessary data transfer is done in conditions of strict security and among a strictly specified number of parties;
- provide an unambiguous explanation in privacy policies with regard to data processing activities including but not limited to data collection by third parties;
- refrain from using data for any other purpose than the one for which it was collected;
- store data exclusively on servers that satisfy adequate privacy and security requirements, and, wherever possible, on the user's device only;
- prioritise the collection of proximity data via Bluetooth technology, rather than through GPS tracking or through access to telecom data;
- prevent profiling and discrimination based on health status;
- ensure regular independent oversight;
- conduct periodic reporting on the efficiency of the app;
- launch awareness-raising campaigns related to the app's deployment and usage.

3.2. Developers are recommended to:

- apply privacy by default;
- incorporate additional data protection safeguards, as appropriate;
- offer a simple and user-friendly interface (i.e., so that individuals with different levels of digital literacy can use the app in an equally simple manner);
- be mindful of accessibility issues;
- ensure technical and functional interoperability with other apps, including by offering multilingual functionality to allow interoperability of apps between countries;
- provide constant technical support (flexible apps prone to improvement based on newly identified challenges);
- add a waiver, in case that the app has a proximity tracking option, that the situation perceived by the app doesn't necessarily reflect the real situation[6];
- involve privacy and health experts in designing apps (when/if applicable);
- conduct a human rights impact assessment prior to the app launch and ensure further regular assessments;
- ensure transparency by informing the user on all aspects related to data collection, usage, and storage, and do so in a friendly and easy to read manner;
- comply with cybersecurity standards and regulations;
- ensure the security of the app and of the collected data through the whole process until their deletion (using methods such as encryption, pseudonymisation, anonymisation);
- put in place a feedback system and provide options for external review.

4. Annex: Overview of COVID-19 tracking apps in SEE+

[6] One of the examples would be a false positive in case a person with symptoms and another app user are closer than two meters, but have a wall or a ceiling between them. The system based on bluetooth would consider it a contact even though it is not. On the other hand, contact tracing relies on the likelihood that two people passing one another have both installed the app on their phones, which can further result in a feeling that an area is COVID free, when in reality it is not. Finally, if an app is oversensitive to contact tracing, it can send a large number of alerts that after some time will be disregarded by a user.