1. Motivation

Das Erfassen und Nachverfolgen von Kontakten und damit möglichen Infektionen durch das Zusammentreffen von SARS-CoV-2 Erkrankten mit anderen, könnte die Ausbreitungsgeschwindigkeit der Pandemie erheblich reduzieren. Eine zentrale Verfolgung mittels Mobiltelefonen erscheint zwar technisch möglich, bringt aber erhebliche Bedenken bezüglich des Datenschutzes mit sich. Der Staat oder wer auch immer diese Daten erfassen und auswerten würde, wäre in einer Position, eine Totalüberwachung der Bürger durchführen zu können. Außerdem würde dies möglicherweise einen Präzedenzfall für andere, möglicherweise weniger dringliche Fälle, bieten.

Es ist jedoch auch möglich eine effektive und effiziente Nachverfolgung zu erreichen und gleichzeitig die Privatsphäre der Teilnehmer komplett zu wahren, indem man die Betroffenen einbindet. Die vorgestellte Lösung sollte so den Datenschutzvorschriften der EU-DSGVO gerecht werden

2. Anforderungen

1. Die Anwendung soll auf effiziente und effektive Weise die Identifikation von Zusammentreffen einer infektiösen Person und mit anderen Personen erkennen und letztere motivieren sich auf eine Infektion testen zu lassen um die Ausbreitung der Pandemie wirksam eindämmen zu können.
2. Der Vorgang sollte soweit erforderlich und wünschenswert automatisiert ablaufen. Die Anwender sollen aber auch selbst in den Prozess involviert werden.
3. Die Privatsphäre der Personen soll so weit wie irgendwie möglich und erforderlich geschützt werden.
4. Es soll nicht möglich sein das Verhalten der Anwender bzw. die Aufenthaltsorte der Anwender zentral nachverfolgen zu können.

3. Methode

Auf jedem Handy eines Teilnehmers würde eine Anwendung installiert, die kontinuierlich Signale auf der Bluetooth-Schnittstelle überwacht. Nähern sich zwei Teilnehmer mit einer solchen App an, so tauschen diese Informationen aus.

Dazu wurde bei der Installation der App ein geheimer Schlüssel erzeugt und zusätzlich dazu erzeugt jedes Mobiltelefon in bestimmten Abständen, z.B. stündlich, einen zufälligen Zahlencode als temporäre ID.

Bei Annäherung tauschen die Mobiltelefone ihren temporäre ID[1] aus und dazu übermittelt jedes Mobiltelefon dem Anderen seine verschlüsselte Position[2] und ggf. noch

[1] Z.B. eine 20-stellige Zahl.

einen genaueren über NFC ermittelter Abstand zwischen den Parteien. Die Mobiltelefone speichern die Daten in einer lokalen Datenbank[3].

- der Zeitpunkte, zu dem der Austausch stattgefunden hat,
- die eigene temporäre ID,
- die temporäre ID der anderen Person sowie
- die von der anderen Person verschlüsselte Position und
- sofern möglich den ermittelten Abstand.

Aufgrund des temporären Charakters der IDs und der verschlüsselten Positionen sind die Einträge in der Datenbank weitestgehend anonymisiert zu bewerten.

Wird nun eine Person positiv auf Covid19 getestet, so können Teile der Daten dieser Person mit Hilfe einer vertrauenswürdigen Institution, z.B. der behandelnde Stelle oder das Analyse-Labor, ausgelesen und in eine öffentlich einsehbare Datenbank übertragen werden. Diese Daten würden über den potentiell infektiösen Zeitraum

- die Zeitpunkte, zu denen der Austausch stattgefunden hat,
- die dazugehörigen verschlüsselten Positionen
- die dazugehörigen eigenen temporären IDs und
- die dazugehörigen temporären IDs der Kommunikationspartner

enthalten. Optional sind noch weitere Informationen denkbar, wie der Abstand oder Informationen zu der infektiösen Person wie Alter oder Geschlecht[4]. Den Umfang dieser Umfang dieser Information kann die vertrauenswürdigen Institution oder die zuständigen Datenschutzbehörden aufgrund datenschutzrechtlicher Grundsätze bestimmen. Wichtig ist dabei, dass aus den veröffentlichten Daten nur die jeweilige andere Kontaktperson die genauen Positionen entschlüsseln kann.

Personen können so über einfache Datenbankabfragen nach den eigenen temporären IDs und den dazugehörigen Zeitpunkten feststellen, ob sie sich in der Nähe einer infektiösen Person aufgehalten haben. Diese Abfrage können regelmäßig und automatisiert erfolgen. Über einen Algorithmus wird anhand der Dauer und ggf. den Abstand des Zusammentreffens ein Infektionsrisiko ermittelt. Ab einem gewissen Schwellwert die Person von der App auf dieses Risiko hingewiesen. In einem noch zu bestimmenden Umfang wird die Person über ungefähren Ort und Zeitpunkt de potentiell infektiösen Aufeinandertreffens sowie ggf. weiteren Informationen zur der infektiösen Person informiert. Anhand der so erhaltenen Informationen kann jede betroffene Person entscheiden, ob sie einen Test auf eine Covid-19 Infektion wünscht.

---

[3] Um Fehler bei der späteren Zuordnung zu vermeiden sollten die Mobiltelefone ihre gespeicherten Daten zu Uhrzeit, Position und Abstand in geeigneter Weise abgleichen

[4] Wird die Verschlüsselung als Public-Key Verschlüsselung mit temporären Schlüsselpaaren ausgeführt, ist es möglich die Zusatzinformationen zu der infektiösen Person zielgerichtet nur den Betroffenen zu Verfügung zu stellen

4. Wesentliche Aspekte

Positive Aspekte

- Die Involvierung der Betroffenen führt zu einer zielgerichteten Identifikation der potentiell infektiösen Aufeinandertreffen, vermutlich besser als dies über eine zentralisierte Anwendung möglich wäre. So kann die betroffene Person anhand der genaueren Umstände, soweit sie diese noch erinnert, entscheiden. Sie könnte ja zu dem Zeitpunkt eine Schutzausrüstung getragen haben, oder sich vielleicht erinnern, dass jemand in ihrer unmittelbaren Nähe gehustet hat oder ihr etwas überreicht hat.
- Die Benachrichtigung der Betroffenen kann sehr zeitnah automatisiert über die App erfolgen

Datenschutzrechtliche Bedenken

- Die betroffene und möglicherweise infizierte Person kann evtl. anhand der Angaben über Ort und Zeitpunkt des Zusammentreffens die infizierende Partei identifizieren. Dies Problem lässt sich aber grundsätzlich nicht vollkommen lösen. Die Verarbeitung sollte durch DSGVO Art. 6 Abs. 1 d) (lebenswichtiges Interesse) und e) (öffentliches Interesse) sowie evtl. b) (Gesetz) abgedeckt sein.
- Dritte könnten die Anwendung nutzen, um anhand von Abfragen unter Angabe von falschen temporäre IDs unberechtigt Informationen zu erhalten. Da die Positionen jedoch verschlüsselt sind und die temporären IDs regelmäßig gewechselt werden, ist der Informationsgehalt sehr gering. Eine Verknüpfung mit anderweitig gesammelten Daten, z.B. solchen die anhand einer selbst betriebenen App an verkehrsreichen Punkten erfasst wurden, wäre eine Identifikation grundsätzlich möglich. Letztlich unterscheidet sich dies aber nicht von den (ungesetzlichen) technischen Möglichkeiten einer Verfolgung von Personen im öffentlichen Raum, wenn diese die Drahtlos-Schnittstellen ihres Mobiltelefons aktiviert haben.