IDAs holdning til

digitale overvågningsredskaber under covid-19

IDA anbefaler:

At der udvikles nationale digitale overvågningsredskaber, her efter overvågningsapps, til bekæmpelse/overvågning af covid-19 i Danmark, hvis der er sundhedsfagligt belæg for, at det ér et effektivt redskab, hvis disse overvågningsapps kan leve op til en række krav og kriterier for it-sikkerhed og privacy, og at det hele tiden er en forudsætning, at der er tale om meget tidsbegrænsede tiltag.

- Det skal være en forudsætning for udvikling og implementering af enhver app eller lign. redskab, at formålet med app'en er præcist formuleret og at designet er tilpasset app'ens formål.
- Indsamling og brug af data skal være videnskabeligt – og ikke politisk – begrundet, dvs. at der kun skal indsamles og benyttes data, der opfylder sundhedsvæsenets specifikt udtalte behov for viden.
- Der skal altid indsamles den mindst mulige mængde data og kun til det oprindelige formål.
- Der skal altid sikres anonymitet til borgere, der bruger app'en og app'en skal være transparent.
- Der skal altid være en tidsbegrænsning for opbevaring og brug af data – en såkaldt solnedgangsklausul. Og der skal udpeges en specifik tilsynsmyndighed, som har til opgave at sikre, at alt data slettes på rette tidspunkt, f.eks. Rigsrevisionen.
- En løsning skal udarbejdes under inddragelse af uafhængige juridiske privacy eksperter og it-specialister indenfor it-sikkerhed, alternativt sendes i høring.
- Download og brug af app'en skal være frivillig.
- Data skal opbevares hos borgeren. Oplysninger om positive testresultater skal opbevares hos en dansk myndighed og altid i Danmark.
- Som borger skal man vide præcist, hvilke data, der bliver indsamlet om én, og man skal når som helst kunne slette app og egne data.
- Oplysninger om, at brugeren er smittet med covid-19, skal være valideret af sundhedsmyndighederne for at undgå fejl og misbrug.

Nødvendigt med præcision af formål

Det første spørgsmål man skal stille sig er, hvorfor app'en er skabt, og hvad den skal bruges til. Et overordnet formål med at overvåge smittespredning af covid-19 bør være at sikre overblik og kontrol med smitteudbredelsen. Det giver en mulighed for hurtigere at åbne samfundet op og dermed være med til at afbøde de menneskelige og økonomiske omkostninger, vi allerede har set i forbindelse med covid-19 pandemien, både i Danmark og på verdensplan. IDA anbefaler, at man bruger den teknologiske udvikling til at understøtte en sådan kontrol, men IDA påpeger også, at sådanne akutte tiltag ikke må underminere den individuelle borgers ret til privatliv og kontrol over egne data. Grundlæggende er IDA forbeholden for ibrugtagningen af overvågningsredskaber til at løse specifikke samfundsproblemer, da det har vist sig at kunne få præcedensvirkning for, hvordan vi i fremtiden kan bruge borgernes data. Der er derfor tale om en unik anbefaling.

Et formål med en app kan være, at man ønsker viden om befolkningens færden, f.eks. mængden af mennesker, der bevæger sig fra en del af landet til en anden for derved at kunne udarbejde modeller for geografisk smittespredning. Det kan også være, at man ønsker at lokalisere særlige steder, hvor der færdes uforholdsmæssigt mange mennesker. I så fald skal app'en indsamle lokationsdata, f.eks. via gps eller telelokation. Det er her ikke nødvendigt med informationer om enkeltindividers færden, derimod kan myndighederne nøjes med datasæt over større grupper af anonyme borgere. At arbejde med større datasæt er med til at sikre borgernes anonymitet i overvågningen.

Men det kan også være et formål at afdække smittekæden fra person til person. I så fald er det ikke relevant at vide, hvor folk har været, men at de har været et sted samtidig med en smittet person – indenfor 2 meters afstand og i mere end 15 minutter. Der vil i dette tilfælde være behov for kontaktsporingsdata, f.eks. via bluetooth, mens information om, hvor kontakten er foregået, ikke behøver at tilgå myndighederne.

Det er altså vigtigt at være præcise med formålet med app'en, så man undgår at indsamle mere end de nødvendige oplysninger.

Grundlaget for indsamling og bearbejdning af data skal være videnskabeligt begrundet

Formålet med udviklingen af en app skal være videnskabeligt og ikke politisk begrundet. Det er afgørende vigtigt for bekæmpelsen af covid-19, at borgerne har tillid til, at de tiltag som myndighederne iværksætter, er funderet i sundhedsvæsenets behov for at kontrollere og nedkæmpe pandemien. Der bør ikke være tvivl om, om overvågningen også – fordi nu har man den jo – bruges til andre formål som f.eks. kriminalitets- eller terrorbekæmpelse. Hvis borgerne mister tilliden til myndighedernes formål med overvågningen, så forsvinder opbakningen til at bruge en app og dermed mister man effekten. I Singapore har kun 6% af befolkningen, på trods af kampagner, downloadet den kontaktsporingsapp, som man lancerede i marts måned og dermed er app'en et ringe bidrag til kampen mod covid-19. For at en app skal have en reel effekt, skal minimum 60 % af befolkningen bruge appen.

Der skal altid indsamles den mindst mulige mængde data.

IDA mener, i overensstemmelse med bl.a. EDPB, European Data Protection Board[1], at mængden af indsamlede data skal begrænses til et absolut minimum. Det skal ske via Data Protection by Design and by Default. Dvs. at app'en skal bygges til udelukkende at opsamle og videresende de absolut nødvendigste data, ligesom det skal sikres, at app'en ikke kombinerer data med andre data fra brugerens mobiltelefon, f.eks. hvem borgerne kommunikerer med. Heller ikke i myndighedernes varetægt bør de indsamlede data sammenkøres med andre personlige oplysningerne om borgeren, medmindre det videnskabeligt kan begrundes som nødvendigt for formålet med app'en.

Det er desuden afgørende for tilliden til en app, at data kun bruges til det oprindeligt aftalte formål.

Registrerede borgere bør altid sikres anonymitet og transparens

For at sikre de registreredes rettigheder, skal app'en udvikles med Privacy by Design for øje.

[1] EDPB, European Data Portection Board "Guidelines 04/2020 on the use of location data and contact tracking tools in the context of the covid-19 outbreak", adopted on 21. April 2020

En af de løsninger, der imødekommer dette, tildeler den registrerede et ikke personhenførbart ID ved oprettelse. Herefter tildeles det ikke-personhenførbare ID et nyt ID hvert femte minut, som interagerer med andre registrerede. Hvis løsningen bygges på, at en server lagrer data, kræver det, at serveren er forsvarligt beskyttet it-sikkerhedsmæssigt, og at det er strengt begrænset, hvem der har adgang til data på serveren. På samme måde bør en tilsynsmyndighed efter et passende tidsrum have adgang til serveren og kunne checke at data slettes – i Norge er det f.eks. 30 dage.

En metode til at sikre anonymitet er, at data forbliver på borgerens mobiltelefon, indtil de faktisk skal i brug, f.eks. hvis man bliver testet positiv for covid-19 og andre borgere, man har været i kontakt med, skal advares. Indsamles data centralt, er det absolut nødvendigt, at it-sikkerheden er i orden. Den norske app, der kun har været på gaden i ganske kort tid, er allerede blevet udsat for succesfulde hackerangreb. Da udviklingen af apps til bekæmpelse af covid-19 sker under ekstremt tidspres, er risikoen for sikkerhedsbrister større end normalt. Dette bør medtages i vurderingen af appens mulige positive effekt.

En måde at sikre transparens i forhold til, hvem der har adgang til data, hvordan og hvor længe og om data er anonyme og faktisk bliver slettet til tiden, er gennem brug open source. En 100% open source baseret app vil være fuldstændig transparent og giver desuden bedre mulighed for at finde fejl og huller, der giver risiko for hacking. Transparens er med til at styrke både tilliden til og sikkerheden ved en app.

Ved eventuel videregivelse af data til andre myndigheder eller forskningsbrug er det afgørende for anonymiteten, at der arbejdes med aggregerede datasæt. Jo større datasæt, der arbejdes med, jo mindre er risikoen for re-identifikation at den enkelte borger.

En solnedsgangsklausul er obligatorisk.

Covid-19 pandemien har sat verden under pres, som det ikke er sket i årtier. Der er imidlertid tale om en akut situation, som formentlig vil være afværget væsentligt inden for nogle måneder – modsat f.eks. klimakrisen, der synes at være en mere eller mindre kronisk tilstand. Det er derfor vigtigt – og en forudsætning for accepten af nødlove og særlige forbud og krav – at de tiltag, der bliver opfundet og udviklet til bekæmpelse af covid-19 behandles som kriseredskaber. Kriseredskaber, der udelukkende bruges under ganske særlige omstændigheder og sættes ud af kraft, så snart vi nærmer os en mindre akut nødsituation. De overvågningsredskaber, der ekstraordinært accepteres i disse måneder, bør på ingen måde blive den nye normaltilstand. Det betyder, at den overvågning og den indsamling af data, som indsamles i denne særlige situation, skal have en klar og på forhånd fastsat udløbsdato, en såkaldt solnedgangsklausul. I den norske app slettes personhenførbare data f.eks. automatisk efter 30 dage, mens et aggregeret datasæt bevares til forskningsbrug.

Der skal udpeges en specifik tilsynsmyndighed, som har til opgave at sikre, at alt data slettes på det fastlagte tidspunkt. Det kan f.eks. være Rigsrevisionen.

En løsning skal sikres via inddragelse af uafhængige juridiske privacy eksperter og it-specialister indenfor it-sikkerhed.

Det er afgørende for effektiviteten af en app, at den downloades af mindst 60 % af befolkningen. Det er derfor nødvendigt, at der er en meget høj grad af tillid omkring app'en. Som nævnt blev den norske app meget hurtigt afsløret som mulig at hacke. Selvom det var et venligtsindet angreb og hullet blev lukket uden, at der skete skade, så viser hændelsen, at der bør være relevant ekspertinddragelse i udarbejdelsen af

app'en. Det er IDAs holdning, at det er nødvendigt at inddrage uafhængige eksperter i test af app'en, inden det frigives.

Indsamling af data og brug af app'en skal være frivilligt

Et kriseredskab som f.eks. apps til overvågning af covid-19, bør være af så god kvalitet og baseret på en så høj grad af tillid, at det kan fungere som et frivilligt redskab, på samme måde som danskerne følger myndighedernes anvisninger uden det store behov for myndighedskontrol. De skandinaviske samfund er præget af en – sammenlignet med andre lande – meget høj grad af tillid til myndighederne. Den norske app, som stadig er i udviklingsfasen, er allerede blevet downloadet af 1,4 mio. ud af 5,36 mio. nordmænd. De første 600.000 downloads skete allerede indenfor det første døgn[2]. Der må forventes, at der også er god basis for at kunne udbrede denne type redskaber i Danmark.

Iflg. EU Kommissionen kan indsamling af data til kontakt sporing, f.eks. til afdækning af smittekæder, kun legitimeres ved frivillighed.

Det er IDAs holdning, at data om borgeren tilhører borgeren selv og at en borger når som helst kan slette app og egne data.

Data skal opbevares hos borgeren. Oplysninger om positive testresultater skal opbevares hos en dansk myndighed og altid i Danmark.

Central opbevaring af data via overvågningstiltag som de foreslåede apps, giver en forhøjet risiko både it-sikkerhedsmæssigt og i forhold til misbrug af data. Data bør derfor forblive hos den enkelte borger.

Hvis formålet er at indsamle lokationsdata, er det iflg. lovgivningen kun anonymiserede datasæt, der bør videregives til myndighederne.

Oplysninger om positive testresultater skal opbevares hos en dansk myndighed og altid i Danmark. Der bør under ingen omstændigheder være data, der overgår til virksomheder eller lande udenfor EU.

Som borger skal man vide, hvilke data, der indsamles og kunne slette dem

Det er afgørende for tillid til en app, at man som borger har let ved at gennemskue, hvilke data, der indsamles om én og hvad de bliver brugt til. Det er IDAs grundlæggende holdning, at data om borgeren tilhører borgeren selv og som borger skal man derfor også når som helst skal kunne slette app og egne data.

Oplysninger om smitte med covid-19 skal være korrekte og godkendt at sundhedsmyndighederne

En af de ting, der adskiller covid-19 fra de almindelige typer influenza vi kender, er smitterisiko allerede inden man får symptomer. Det kan derfor give mening, at man kan spore tilbage de mennesker, man har været i nærheden af, defineret som indenfor 2 meters afstand i mere end 15 minutter, i dagene op til, at man er testet positiv. Det gælder også mennesker, man ikke kender, men har været i nærheden af i f.eks. supermarkeder eller i den offentlige transport. Det forventes herefter, at disse mennesker skal gå i

[2] Trond Markussen, formand for NITO på webinar 23.april 2020: https://ida.dk/viden-og-netvaerk/videoer-fra-ida/european-approaches-to-data-surveillance-and-tracking-in-the-light-of-covid-19

karantæne og lade sig teste, inden de f.eks. fortsætter med at gå på arbejde, hente børn, købe ind etc. Det er altså ikke uden omkostninger, at man modtager en advarsel om, at man for længe har været for tæt på et menneske, der har vist sig at være smittet. Et advarselssystem bør derfor være kendetegnet ved en høj kvalitetssikring af data. Denne kvalitetssikring bør ske ved, at myndighederne godkender en person som smittebærer, inden personen kan vælge at registrere sig som smittebærer. Alternativet er en risiko for, at nogen for sjov eller for at skade, anmelder sig selv om smittebærer uden at være det.

En måde at håndtere dette på kunne være, at sundhedsmyndighederne kan aktivere en funktion på en borgers app, der giver mulighed for at advare andre, når man er blevet testet positiv. Derefter kan borgeren aktivere en advarsel, der sendes ud til de ID-adresser, man har været i nærheden af uden at sundhedsmyndighederne i øvrigt behøver at få adgang til eller viden om, hvilke ID-adresser, ens telefon kommunikerer med. Denne løsning er inspireret af forslag fra it-miljøet, se illustration nedenfor, men med den tilføjelse, at det er sundhedsmyndighederne, der åbner op for, at borgeren kan sende informationen om smitte (som nu igen anonymiseres, jf. tegningen) videre til et hospital eller anden institution.

I en dansk model bør det være sundhedsmyndighederne, der giver Alice mulighed for at sende informationer videre til "hospitalet", for at sikre validering af, hvem der faktisk er testet positive.