



Etiske hensyn ved digital kontaktopsporing

Hvis man kan opspore virus i takt med at det bevæger sig rundt i befolkningen, er håbet at man kan opretholde en hverdag og holde smittefaren på et acceptabelt niveau. Så skal vi øge overvågningen og bruge data om befolkningens adfærd for at holde samfundet åbent og smitten nede?

OM MATERIALET

Denne tekst er udarbejdet af en styregruppe bestående af følgende rådsmedlemmer:

Henrik Nannestad Jørgensen, Jacob Giehm Mikkelsen, Lise Müller, Mette Reissmann, Eske Willerslev

Projektleder: Frank Beck Lassen

Teksten er en del af Det Etiske Råd tema om COVID-19 og etik. Find det samlede materiale på rådets hjemmeside: www.etiskraad.dk/covid

Teksten er senest revideret 17. juni 2020



**DET
ETISKE
RÅD**

OPSPOR, TEST, ISOLÉR

Meget tyder på, at vi skal leve med COVID-19 som en del af samfundslivet i længere tid. Et redskab til at undgå en genopblussen af epidemien kunne være kontaktopsporing: en hurtig identificering og karantæne af smittede individer, opsporing af hvem, de har haft tæt kontakt med, og desinfektion af de steder, de smittede har været.

Kontaktopsporing har hidtil været foretaget manuelt. Ved at interviewe patienter, forsøger man at identificere de personer, der har haft kontakt med dem i den periode, hvor de regnes for smittebærere. Denne form for kontaktopsporing fremviser muligvis gode resultater, men er også et arbejde, som kræver stor tålmodighed, præcision og timing i indsats for at virke. Det kræver en omfattende arbejdsindsats og afhænger af aktørers vekslende hukommelse.

Forhåbningen til digital kontaktopsporing er, at en smartphone kan omgå en række af disse udfordringer, når det gælder tempo, rækkevidde og præcision. Den største fordel ved introduktionen af en digital opsporingsevne er således, at man kan fokusere mere på *specifik kontakt frem for generel karantæne*.

En generel karantæne som den vi i Danmark har gennemlevet, er en effektiv men upræcis måde at reducere spredningen af smitte og dermed sikre sundhedsvæsenets kapacitet og evne til at kunne behandle de, der er kritisk syge af COVID-19. 'Nedlukning' udgør desværre også et voldsomt indgreb i borgernes bevægelsesfrihed og ret til at forsamle sig, samt i befolkningens produktivitet, markeders effektivitet og virksomheders omsætning. Indgreb i borgerrettigheder er altid bekymrende, mens arbejdsløshed, frygt og social isolation frygtes at have store sundhedsmæssige konsekvenser for befolkningen.

Det endelige formål med en generel karantæne er at reducere kontaktraten. Karantæne er således ikke et formål i sig selv, men et middel, vi anvender, når vi ikke besidder andre. Interessen samler sig derfor om de kontakter, de smittede har haft. Ved at forstå, hvorledes smittede har haft kontakt med ikke-smittede, kan der udvikles strategier for brugen af ressourcer, for hvem der skal kontaktes, testes og måske sættes i karantæne. Set fra et samfundsøkonomisk og sundhedsfagligt synspunkt kan der være store gevinster herved.

Uheldigvis kan de samme digitale kontaktopsporingsredskaber, som tænkes anvendt i forbindelse med epidemier som COVID-19, også bruges – og er i nogle lande blevet brugt – til at udvide masseovervågning, begrænse individuel frihed og offentliggøre private detaljer om enkeltpersoner.

TEKNOLOGIEN BAG KONTAKTOPSPORING

Groft sagt lader brugen af digital teknologi og data til kontaktopsporing sig inddele i tre kategorier. De, der opsamler, de, der overvåger og evt. vurderer, og de, der håndhæver. Der findes således:

- Apps der *opsamler* data til at dokumentere spredningen af virus og vurdere effekten af samfundsmæssige tiltag. En række store techselskaber som Google, Facebook og

Apple ved allerede, hvor vi befinder os, og kan således generere data, der viser effekten af nedlukningen af samfundet.

- Apps der kan hjælpe borgere eller myndigheder med at *overvåge og vurdere*, hvor smitteudsatte personer har været, måske hjælpe personer til at vurdere deres egen helbredstilstand, eller endda opfordre eller afkræve, at man opsøger en testfacilitet eller går i karantæne. Den nævnte kinesiske app Alipay Health Code, med dens rød, gul, grøn indikatorer er et eksempel.
- Apps der *håndhæver* en karantæne. I Hongkong har man bedt smitteramte borgere om at gå i karantæne og tænde for lokationsfunktionen på WhatsApp, hvorefter myndighederne kan overvåge, om borgeren bryder karantænen. I Singapore har man udviklet en specifik app til dette formål, mens man i Taiwan har valgt at indhente data fra mobilmaster for på den måde at følge borgernes og de karantæneramtes bevægelser.

I forhold til overvågning med henblik på kontaktopsporing findes der forskellige teknologiske muligheder.

Det er muligt direkte at indhente lokationsdata fra mobilmaster eller teleudbydere. Gøres dette, vil man (afhængig af lovgivning) som myndighed eller privat aktør have stor kontrol over data og kan indhente data uden borgernes viden eller samtykke. I lande med strengere samtykkelovgivning er det muligt at bede teleoperatører om at udlevere anonyme, aggregerede data, som de allerede er i besiddelse af. I Danmark har teleselskaber siden 6. april udleveret teledata i anonym og aggregeret form til SSI via Danmarks Statistik.

En anden model er at bruge mobiltelefoners GPS-data, en model, som anvendes af både større og mindre teknologivirksomheder. GPS-data er dog svære at anonymisere og medfører derfor privatlivsudfordringer.

Endelig er det muligt at anvende Bluetooth-teknologi. Brugeren installerer en app og tænder for Bluetooth-funktionen. Herefter registrerer app'en hver gang, den er i nærheden af en anden telefon, der også har installeret app'en. Data registreres i krypteret form på telefonen og deles altså ikke med en central enhed. Skulle en bruger af app'en blive smittet, kan vedkommende vælge at registrere sig selv som smittet, hvorefter alle registrerede kontakter bliver notificeret.

Fordelen ved den sidste model er, at der kun benyttes kontaktdata og ikke brugernes geografiske positioner samtidig med at disse kan lagres lokalt på mobiltelefoner, fremfor i et centralt datalager. Et centralt punkt bliver da, om data automatisk videregives til

et centralt datalager for opbevaring og videre analyse, eller om det kun kan foregå ved brugerens samtykke.

Endelig skal det nævnes, at en virkningsfuld app i fremtiden skal benytte sig af en fælles bagvedliggende platform, udviklet af internationale, private virksomheder. Det vil være af stor betydning, at der er gennemsigtighed omkring udviklingen af en sådan platform.



Vigtige beslutninger om nye digitale tiltag bør ikke træffes under kritiske og accelererede forhold – og det er ikke uset, at kortsigtede krisetiltag efterfølgende bliver permanente løsninger

ETISKE OPMÆRKSOMHEDSPUNKTER

Tiltag såsom overvågning, obligatorisk behandling, vaccination, isolering og karantæne kan i nødsituationer vise sig nødvendige af hensyn til den almene sundhed: Det kan derfor med rimelighed føre til begrænsninger i basale frihedsrettigheder såsom retten til privatliv, samtykke til behandling og bevægelsesfrihed.

Den nuværende krise fremhæver et klassisk trade-off mellem personlige friheder og den offentlige sikkerhed. I et stadigt mere digitalt samfund som det danske, med dets muligheder for opsporing og prognosedannelse, skærpes dette dilemma: Hvordan skal afvejningen mellem privatliv og den almene sundhed se ud?

Privatliv er essentielt for individet, da det af mange anses for en betingelse for at kunne bevare forskellige typer af sociale relationer til andre mennesker. At have et privatliv er en forudsætning for intimitet, for at kunne trække sig tilbage, ja for at kunne tænke frit.

Indgreb i privatlivet gennem kontaktopsporing og profilering lader sig derfor vanskeligt retfærdiggøre, medmindre det som minimum er indbygget i systemerne, at data kun bruges til de specifikke sundhedsudfordringer, der er for hånden. Overvågning, frivillig eller påtvungen, lader sig muligvis retfærdiggøre, men kun hvis det har til formål at reducere morbiditet og mortalitet og ikke, hvis det er ledsaget af straffende foranstaltninger.

Selvom rettigheder som bevægelsesfrihed og privatliv er vigtige, kan de altså blive trumfet af sikkerhedshensyn, når trusler mod samfundet som helhed er tilstrækkeligt store. Den amerikanske filosof Ronald Dworkin har således foreslået en tommelfingerregel, som understreger: *Hvis handlinger er umoralske, så tæller friheden til at forfølge dem for mindre*. Risikerer du at smitte dødeligt sårbare grupper ved at insistere på din uregistrerede bevægelsesfrihed og ret til privatliv, tæller disse rettigheder mindre.

På den anden side bør der være stærke beviser for, at meget indgribende sundhedstiltag også (og alene) virker i den sammenhæng, de er tiltænkt. Nancy Kass har formuleret en

tommelfingerregel, som lyder: *Jo større byrder en sundhedsteknologi pålægger befolkningen i form af udgifter eller indgreb i frihedsrettigheder, desto stærkere beviser må der være for, at teknologien vil opnå dets mål.*

Som de to tommelfingerregler antyder, skal der findes en balance mellem frihed og sikkerhed. Hvor meget frihed er det rimeligt for individet at opgive for at vinde en yderligere sikkerhed? Et sådant spørgsmål angår hvad vi ofte kalder for 'privatlivets fred', men måske introduktionen af digital kontaktopsporing handler om mere end hvorvidt en app begrænser den enkelte i at gøre som man måtte ønske.

Det er værd at overveje, om der muligvis også er en mere overordnet samfundsinteresse i spil, der handler om graden af mulig privatliv for alle borgere. Måske beskyttelsen af privatlivet ikke blot er en individuel ret, men et kollektivt gode. I et sådant perspektiv berører introduktionen af en statslig drevet kontaktopsporingstjeneste ikke kun 'berørte individer', men alle borgeres virkelighed og oplevelse af at blive overvåget. I forbindelse med digital kontaktopsporing er der en række forhold at være opmærksom på:

Moden overvejelse

Man bør overveje, om vi i en kritisk situation efterspørger en tilbagevenden til normalitet så meget, at vi risikerer at ofre grundlæggende borgerrettigheder for en uvis teknologisk gevinst. Vigtige beslutninger om nye digitale tiltag bør ikke træffes under kritiske og accelererede forhold – og det er ikke uset, at kortsigtede krisetiltag efterfølgende bliver permanente løsninger. Kriser kan siges at accelerere politiske og teknologiske processer. Beslutninger, som det normalt ville tage mange år at teste og reflektere over, vedtages på få dage eller uger. Det øger risikoen for, at umodne eller uigennemtænkte teknologier tages i brug, når risikoen ved ikke at gøre noget føles større.

Effektivitet

Man bør overveje, hvor effektive disse teknologier vil være. Da digital kontaktopsporing bruger en smartphone eller lignende som en 'erstatning' for registreret kontakt, kan de give anledning til unøjagtigheder og dermed levere et misvisende billede af sygdomsudbredelsen. Desuden er den kontakt, en telefon kan påvise, ikke lig med COVID-19's virkelige opførsel. Det er muligt at sidde få meter fra nogen uden at blive smittet, for derefter at blive smittet ved at sidde i et togsæde benyttet af en smittet flere timer før. Endelig bør man huske, at der er mange, der ikke ejer en smartphone eller ikke bærer den på sig hele tiden.

En virkningsfuld digital løsning afhænger derfor af mange ikke-teknologiske faktorer. Hvis digital kontaktopsporing skal være en succes, kræver det et holistisk syn på overvågende teknologier i sundhedsøjemed. Vi har fx endnu til gode at se, hvilke resultater vi i Danmark kunne have opnået med manuel smitteopsporing eller et velforberedt beredskab. Det bør derfor overvejes, hvilket samarbejde en smitteopsporingsapp skal have med manuel kontaktopsporing, og om ikke en sådan app kun skal tænkes som et supplement til en bredere indsats. Gennemtænkte organiseringer af arbejdsgange eller tilstrækkelige vejledninger for personale, kan ikke uden videre afløses af en app. Endelig kan en digital smitteopsporing naturligvis kun udrulles i sammenhæng med, at der er

tilstrækkelig testkapacitet og at der er tilstrækkelig mulighed for manuelt at følge op på det øgede behov for test, registrering og isolering, som en succesrig app vil generere.

Som supplement ville en smitteopsporingsapp muligvis øge opmærksomheden på eget ansvar for smitte. Hvis der er en forpligtelse til at give sig til kende som smittet, så kunne en sådan app hjælpe med at leve op til den forpligtelse.

Proportionalitet

I sammenhæng med spørgsmålet om, hvor virkningsfuldt digital kontaktopsporing vil være, bør man overveje, om der er proportionalitet i løsningerne. Her opstår store spørgsmål om sikringen af de juridiske rammer for en overvågning af denne karakter. Opsporingen af personer, der kunne være smittet med COVID-19, vil kræve lovgivning, der specificerer, hvordan dataindsamlingen skal foregå, hvor længe den skal foregå og hvilke sundhedsformål, der er relevante.

Realistiske bedømmelser af effektivitet og proportionalitet er afgørende for legitimitet og modtagelsen af en opsporings-app. Ville mindre indgribende tiltag kunne opnå de samme effekter? Er den tekniske løsning foreslået realistisk og effektiv og vil den bidrage med nogen væsentlig værdi i krisehåndteringen?

Givet den manglende viden om hvor effektiv en digital kontaktopsporing vil være, vil det fx være uforholdsmæssigt indgribende at gøre brugen af en app obligatorisk.

Man bør derfor tage hensyn til, om teknologien står i proportion til problemet. Der skal være et rimeligt forhold mellem det, vi som samfund opnår ved at gribe ind, og de begrænsninger i menneskers frihed, indgrebene medfører.

Det er i den forbindelse vigtigt hele tiden at have det egentlige mål for øje. Målet er ikke alene at kunne sende en sms til potentielt smittede, men i sidste ende at mindske smitte. Sammenlignet med det bør man huske, at der kan være store forskelle i mulighederne for at reagere på en evt. sms. Kan alle selvisolere og arbejde hjemmefra? For mange ansatte vil selvisolering kræve, at man inddrager en arbejdsgiver, og dermed synes privatlivsbeskyttelsen kun at være tilgængelig i praksis for de, som kan arbejde hjemmefra.

Glidning i brugen

Der kan være en tendens til, at teknologier, som er blevet udviklet med ét formål, ofte efterfølgende bruges i andre sammenhænge. Hvis der skabes teknologier til sygdomsovervågning, vil det så regnes for forsvarligt ikke at udnytte de muligheder, som disse teknologier tilbyder?

Et hensyn, der skal tages med i betragtning, vil være, hvordan man sikrer, at digital opsporing ikke breder sig utilsigtet til andre sygdomsområder, som fx almindelig sæsoninfluenza, men også til helt andre dele af samfundet, det være sig afsoning, plejehjem eller opsyn med mindreårige.

En række offentlige myndigheder, beskæftiget med at kontrollere for bedrageri og misbrug af sociale ydelser, kunne have en interesse i at vide hvor mistænkte borgere befin-



Det er derfor vigtigt at overveje, om vi som samfund overhovedet ønsker at gå i en mere digital retning når det gælder bekæmpelsen af virus. Måske er det den allerede eksisterende tillid og ansvarlighed befolkningen imellem, der hjælper i kampen mod virussen

der sig. En digital kontaktopsporing kunne give nye og mere gennemgribende muligheder for at udforske eller modvirke formodet bedrageri.

Kvaliteten af data

Der vil i behandlingen af data være brug for en stærk kvalitetskontrol. Data fra wearables og andre personlige digitale enheder kan introducere en række fejl i datamaterialet, der kan skævvride prognostiske modeller i stor skala. Hvis modelleringer og advarsler er utilstrækkelige, stigmatiserende eller blot fejlagtige, eller ikke tillader at fejlsporinger kan rettes, vil det underminere tilliden til digital opsporing. Ukorrekte data kan give en falsk sikkerhed og opmuntre til en mere risikobetonet adfærd – pårørende kan fx tro sig smittefrie og dermed besøge ældre familiemedlemmer på et forkert grundlag. Modsat kan falske positive meddelelser resultere i en ubegrundet frygt og usikkerhed.

Det er derfor nødvendigt, at det er en sundhedsfaglig afgørelse, om en person skal registreres som smittet. Hvis for mange brugere oplever falske meddelelser, nyttesløse isoleringer, eller at det for tredje gang viser sig, at man ikke var smittet, selvom en app gjorde det sandsynligt, så risikerer opbakningen til digital kontaktopsporing at svinde ind.

Tillid

Overhovedet at få borgere til at deltage og dermed indberette deres smittestatus kan blive en selvstændig udfordring. For at en bluetooth-baseret løsning kan give et retvisende billede af smittekæder eller levere brugbare modeller der forudsiger spredning, kræver det, at mindst 60 % af befolkningen bruger den. En sådan tilslutning opnås kun, hvis der er tillid til den valgte løsning, hvilket sandsynligvis forudsætter, at alle relevante etiske hensyn er taget i betragtning.

Det er derfor vigtigt, at man tager sig tid til at kommunikere formålet med digital opsporing og dokumenterer de godartede virkninger. Hvis ikke der sikres opbakning i befolkningen, så vil det det ikke kun være til skade for en enkelt apps troværdighed, men også kaste skygger over den langsigtede tiltro til digitale sundhedsløsninger.

Digital kontaktopsporing må ikke bidrage til skyldiggørelsen over at være blevet syg, øge fornemmelsen af sårbarhed eller bidrage til et syn på andre borgere som potentielle

smittekilder. Som samfund kæmper vi i forvejen tilstrækkeligt med, at det banale, i form af kontakter, møder, gåture, og lignende, er blevet risikabelt på en ny måde.

Det er derfor vigtigt at overveje, om vi som samfund overhovedet ønsker at gå i en mere digital retning, når det gælder bekæmpelsen af virus. Måske er det den allerede eksisterende tillid og ansvarlighed befolkningen imellem, der hjælper i kampen mod virussen. Hvilken effekt en digital overvågningstilgang vil have på en sådan tillid, kendes ikke.

EKSEMPLER PÅ DIGITAL KONTAKTOPSPORING

Brugen af digital kontaktopsporing er allerede kendt fra udlandet. Her findes der en række eksempler på etisk diskutabile anvendelser af digital kontaktopsporing. I det følgende gives to eksempler på meget vidtgående tiltag samt 7 principper for udviklingen af en dansk app, der er blevet aftalt mellem en bred vifte af Folketingets partier.

Syd Korea: data fra overvågningskameraer, lokationsdata og kreditkortanvendelser

I Syd Korea har myndighederne gjort brug af optagelser fra overvågningskameraer, lokationsdata fra smartphones og kreditkortkøb i forsøget på at opspore smittebærere og smittekæder.

Der er således pligt til at underrette myndighederne om, hvor man har været, hvis man bliver smittet med COVID-19 i Syd Korea. Oplysningerne bliver offentliggjort via myndighedernes hjemmesider og advarselssystemer med oplysninger om fx køn og alder. Rejsende fra lande med smittefare skal downloade en mobilapp i lufthavnen, som skal opdateres med data om, hvor man har været og om mulige symptomer og kropstemperatur.

Syd Koreas model for kontaktopsporing bygger på ”Loven til forebyggelse af og kontrol med infektionssygdomme”. Sundhedsmyndigheder kan med politigodkendelse få adgang til GPS-data, kreditkortoplysninger, rejsehistorik og patientjournaler. Siden slutningen af marts har et nyt system til dataanalyse gjort det muligt at trække disse oplysninger på få minutter for at danne en bevægelsesprofil af enkeltpersoner. Med mobile stationer foretager man kontroller og laver profiler på stedet i risikoområder i Seoul.

Kina: klassificering af borgere i røde, gule og grønne grupper

I Kina har adskillige byer krævet, at borgere anvender software på deres telefon, som klassificerer dem med en farvekode (rød, gul eller grøn) alt efter smittefare. Programmet afgør, hvem der skal i karantæne eller hvem, som får lov at benytte fx offentlig transport. To af de største kinesiske techselskaber, Tencent og Alibaba, har udviklet hver deres app. Tencents version holder øje med, hvor brugeren har befundet sig i de seneste to

uger, og kan således afgøre, om vedkommende har været i et smitteramt område eller om brugeren har været tæt på personer, der senere har vist sig at være smittet.

Danmark: frivillighed, privacy og decentral opbevaring af data

I Danmark har en række af Folketingets partier formuleret syv principper, der skal være bindende for udviklingen af en dansk app designet til kontaktopsporing. Principperne er som følger:

- Appen er baseret på frivillighed
- Brugervenlighed og værdi for borgerne skal sikre kritisk masse
- Data om borgeres kontakter skal alene opbevares decentralt på borgerens egen mobiltelefon – ikke på central server – og data slettes efter 14 dage
- Myndighederne har ikke adgang til personhenførbare data om borgerens kontakter
- Appen følger gældende lovgivning og skal leve op til krav om privacy og sikkerhed
- Appen lukkes ned og alle data slettes, når appen ikke længere er aktuel at bruge i forbindelse med COVID-19
- Muligheden for at anvende appen på tværs af grænser undersøges i samarbejde med EU-lande, så appen om muligt kan understøtte interoperabilitet

Det står klart, at der er væsentlige forskelle på de tre landes tilgange til digital kontaktopsporing. Introduktionen af en app til digital kontaktopsporing udgør et nybrud, både juridisk teknologisk og etisk. På den baggrund er det vigtigt at gøre sig bekendt med de etiske hensyn, da en sådan app muligvis sætter nye standarder for relationen mellem myndigheder og borgere, såvel som mellem borger og borger.

De etiske hensyn forbundet med digital kontaktopsporing er del af en større problematik forbundet med brugen af wearables i sundhedssammenhænge. Det Etiske Råd har i 2019 udtalt sig om "Etik og sundhedsdata". Endvidere præsenteres og diskuteres en række dilemmaer forbundet med wearables i Det Etiske Råds redegørelse Sundhedswearables og big data (find begge udgivelser på www.etiskraad.dk/etik-og-sundhedsdata).