Teknologirådet

DIGITAL SMITTESPORING

Helsemyndighetenes strategi for å åpne opp Norge etter nedstengningen er å gjøre målrettet testing, isolering, smittesporing og karantene.

Smittesporing er viktig, men vanskelig. Vi glemmer raskt hvor vi har vært den siste tiden, og kjenner ofte ikke til hvem vi har vært i nærheten av, for eksempel på bussen. Dessuten har mange som smitter andre få eller ingen symptomer.

Hittil har smittesporing blitt utført som et møysommelig manuelt arbeid, hovedsakelig ved telefonintervjuer. Det skalerer imidlertid dårlig, og er tid- og ressurskrevende.

Digital smittesporing

Smarttelefoner kan registrere hvor man befinner seg, og hvilke andre telefoner som er i nærheten. Ideen bak smittesporings-appene som innføres i mange land er å utnytte denne informasjonen til å spore og varsle mulig smitte. Når en bruker får påvist covid-19-smitte, kan systemet identifisere hvor brukeren har vært, og hvem brukeren har vært i nærkontakt med.

Appene kan straks og automatisk varsle alle nærkontakter som systemet avdekker. En reduksjon i responstid for å spore opp mulige smittede fra dager til minutter, vil kunne hindre antall nye smittede betraktelig.

15. april lanserte norske helsemyndigheter appen Smittestopp, som er utviklet av Simula-senteret. 3. juni var det 592 924 aktive brukere av appen. I første omgang prøves appen ut i noen utvalgte kommuner, bl.a. for å vurdere om appen identifiserer flere nærkontakter enn det som fanges opp manuelt.

SAMMENDRAG

- Digitale smittesporing kan gi tidligere varsling til potensielt smittede, samt kartlegge hvordan sykdom sprer seg og om tiltak virker.
- Nytten av sporings-apper er foreløpig usikker og må vurderes løpende.
- Smittestopp-appen samler og lagrer sensitive data om brukernes smittetilstand, lokasjon, bevegelse og nærkontakter. Bruken er frivillig, tidsbegrenset og data skal slettes.
- Smittestopp har tre ulike formål, men dette er verken spesifisert i forskriften eller i samtykkeerklæringen til innbyggerne.
- Anonyme data fra digital sporing kan re-identifiseres og bør derfor ikke brukes av andre enn helsemyndighetene.
- Norge, Frankrike og Storbritannia har valgt sentralisert lagring av sporingsdata fordi det gir raskere og mer presis smittesporing, mens andre europeiske land har valgt en desentralisert modell av hensyn til personvernet.
- Det er faglig uenighet om åpen kildekode er beste strategi for å gjøre appen sikker.

Personvernhensyn

Smittestopp samler og lagrer brukernes smittetilstand, lokasjon, bevegelse og nærkontakter. Disse dataene er personlige, sensitive og vanskelige å anonymisere. Slike data bør i tråd med personvernforordningen GDPR samles inn i så liten grad som mulig, og beskyttes godt.

Behandling av persondata i Smittestopp er regulert av en ny forskrift for digital smittesporing og epidemikontroll, som varer fra 27. mars til 1. desember 2020.

Mens alle innbyggere som får påvist koronasmitte er påbudt å hjelpe med smittesporing, vil digital smittesporing være frivillig. Brukeren kan skru av sporingen for en periode, og kan når som helst avinstallere appen. Personopplysningene kan ikke benyttes for å kontrollere om enkeltpersoner overholder råd eller pålegg, og heller ikke utnyttes kommersielt.

Lokasjonsdataene vil i følge Folkehelseinstituttet (FHI) bli slettet etter mindre enn 10 dager. Når deltakeren fjerner applikasjonen fra sin mobiltelefon, skal alle personopplysninger om deltakeren slettes eller anonymiseres.

Det forventes at pandemien vil vare lenger enn til 1. desember 2020. Dette reiser spørsmål om kriterier for forlengelse, og hva som definerer at pandemien er over.

Hvor presis blir automatisk varsling?

For at digital smittesporing skal gi merverdi, må smitten begrenses så godt som mulig, med få unødvendige omkostninger, som karantene for friske personer.

Automatisk smittevarsling baserer seg på én felles definisjon av «nærkontakt» for å utløse varselet. Smittestopp bruker definisjonen gitt av Folkehelseinstituttet: Nærkontakt betyr mindre enn 2 meters avstand i mer enn 15 minutter sammenhengende med en person som er bekreftet syk med covid-19.

Smarttelefoner måler ikke nødvendigvis avstand mellom personer. I virkeligheten varierer smittefaren ut fra situasjonen. Dette kan redusere nytten av automatisk smittesporing på to måter:

Lav spesifisitet vil si at mange får varsel selv om de ikke er smittet (falske positive). Skolesekker med telefoner som ligger sammen vil bli målt som nærkontakt, selv om elevene holder avstand. Smarttelefoner vet heller ikke om det er beskyttelsesskjermer, vegger eller gulv mellom nærkontakter. Falske alarmer kan drive opp etterspørselen etter tester og gi unødvendige karantener og frykt i befolkningen.

Lav sensitivitet vil si at mange ikke får varsel selv om de er smittet (falske negative). Smarttelefoner forstår ikke egenskaper ved omgivelsene som kan påvirke smitterisikoen. Dårlig luftventilering på korøvelser kan for eksempel innebære risiko for smitte, selv om avstand og varighet ikke er definert som nærkontakt. Det kan skape falsk trygghet og økt risiko for at smittede personer smitter andre.

I bred forstand er sensitiviteten også avhengig av hvor stor andel av befolkningen som bruker appen. Jo flere bekreftet smittede som bruker Smittestopp, jo flere nærkontakter kan varsles raskt For at mange nok skal laste ned appen, må de oppleve at den treffer godt. Presisjon og utbredelse er derfor gjensidig avhengige størrelser

Gevinsten er usikker

Selv om flere land bruker digital smittesporing, eller har planer om det, er det ennå ikke dokumentert at dette faktisk gir lavere smitte. Norge er tidlig ute, og det bør derfor gjøres kontinuerlige vurderinger av om nytten står i forhold til kostnadene for innbyggerne og samfunnet.

Reglene som definerer nærkontakt må derfor finjusteres etterhvert som det blir mer kunnskap om hvordan koronasmitte skjer, og hvordan mobiltelefonen som sporingsverktøy fungerer i praksis.

Hvor mange av nærkontaktene som er falske positive, er en viktig del av vurderingen. Det bør også gjøres anslag over antall smittede som ikke blir fanget opp av appen.

Anbefalingene i det automatiske varselet bør stå i forhold til hvor spesifikt appen treffer. Det er grunn til å anta at det vil være et betydelig antall falske postive, på grunn av feilkildene. I stedet for å anbefale karantene, kan nærkontakter for eksempel anbefales å teste seg. Slik sett er den viktigste funksjonen til digital smittesporing å bidra til å prioritere hvem som skal testes.

Smittestopp kan også fungere som støtte for manuell smittesporing. Den kan registrere hvor smittede brukere har vært og hvem de har møtt. En menneskelig smittesporer kan luke ut falske positive, og fange opp tilfeller som ellers kunne gått under radaren. Dette vil imidlertid gjøre at andre enn i dag får tilgang til sensititive data fra appen.

Egne samtykker til hvert formål?

Smittestopp har tre distinkte formål. Ifølge forskriften skal den bidra til *rask oppsporing av og formidling av råd* til personer som kan være smittet av koronaviruset SARS CoV-2. Videre skal den gjennom *overvåkning på befolkningsnivå* bidra til å følge smitteutbredelse og

vurdere effekt av smitteverntiltak.

På Simulas hjemmesider utrykkes også et tredje formål utover dette, nemlig å skaffe *anonyme data til forskning*, for å være bedre forberedt på fremtidige pandemier.

De tre formålene kan gi samfunnsmessig gevinst, men hvert formål har behov for ulike typer og mengder data. Det blir vanskelig å vurdere om behandlingen av opplysningene er nødvendig for å oppnå det enkelte formål ettersom FHI ikke har skilt klart mellom dem. Her bør helsemyndighetene beskrive hvilke effekter de ønsker å oppnå for hvert formål, og hvordan de vil bruke ulike typer data til dette.

Brukeren kan i dag kun gi ett samtykke til alle formålene samtidig, og må dermed samtykke til mer utstrakt bruk av data enn kun smittesporing. Det vil styrke personvernet om brukeren kan velge å gi sitt samtykke til de ulike formålene hver for seg.

Videresalg av anonyme data

Ifølge helse- og omsorgsminister Bent Høie er gjenbruk av anonyme data viktig for verdiskapning og innovasjon, og det "er ikke satt konkrete begrensinger i forskriften for videresalg av anonyme, aggregerte data".

I takt med utviklingen av mer intelligente dataanalyser og maskinlæring blir det imidlertid mulig å utlede stadig mer informasjon ved å koble sammen flere datasett som hver for seg har god personvernbeskyttelse. Det kan føre til at anonymiserte datasett blir identifiserbare.

Dersom de anonymiserte dataene kobles med store datasett hos eksempelvis store internasjonale selskaper, kan norske borgere i verste fall re-identifiseres. Videresalg av data fra Smittestopp, også anonyme, bør derfor vurderes på nytt.

Er posisjonsdata nødvendig?

Det er spesielt to måter å registrere nærkontakt på som er aktuelle for digital smitte-sporing:

- Bluetooth er en funksjon i de fleste mobiltelefoner som kan oppdage andre telefoner innenfor en rekkevidde på omtrent 10 meter. Signalstyrken indikerer avstanden.

- GPS *(Global Positioning System)* er et satellittbasert system som kan lokalisere en telefon med en nøyaktighet ned mot 2-7 meter.

Brukeren må aktivt tillate bruk av Bluetooth og GPS-sporing. Smittestopp bruker både GPS og Bluetooth for å beregne nærhet til andre telefoner. Simula mener denne kombinasjonen gir best nøyaktighet. Det europeiske personvernrådet (EDPB) påpeker imidlertid at kontaktsporing ikke krever GPS-sporing av individer og at slik innsamling dermed er i strid med prinsippet om dataminimering. Dataminimering innebærer å begrense mengden innsamlede personopplysninger til det som er nødvendig for å realisere formålet med innsamlingen.

Sentralisert eller desentralisert lagring?

Kontaktdata kan lagres på to ulike måter. I *sentraliserte løsninger* samles informasjon om nærkontakt inn av helsemyndighetene. Når noen får påvist smitte, sender myndighetene umiddelbart et varsel til de som har hatt nærkontakt om mulig smitte. Myndigheter får også mulighet til å følge med på utviklingen og oppdatere sine strategier fortløpende.

Norge bruker en sentralisert løsning, i likhet med Frankrike og Storbritannia. Simula påpeker at bruken av data er godt regulert i forskriften for digital smittesporing og at sentral lagring gir raskere og mer presis smittesporing, bedre forståelse av effekten av ulike tiltak, og forskning for å forstå fremtidige epidemier. Sentralisert lagring kan dessuten være nyttig dersom digital smittesporing skal kombineres med manuelt arbeid.

Desentraliserte løsninger har blitt valgt i andre europeiske land, som Tyskland og Danmark. Informasjon om kontakt kan lagres anonymt og kryptert i hver enkelt brukers mobiltelefon. Når noen får påvist smitte, beregner systemet hvem som skal varsles om mulig smitte i henhold til programmerte regler. Ingen tredjeparter trenger å få innsyn i dataene.

Google og Apple har i samarbeid utviklet en slik løsning som kan varsle nærkontakter mens data kun er tilgjengelige på mobiltelefonene. Den skal også gjøre det mulig å utveksle og måle nærhet mer presist og på tvers av ulike telefoner med Bluetooth. Google og Apple tilbyr et grensesnitt, og hvert land utvikler og drifter sin egen smittesporingsapp. En felles tilnærming vil også ha fordeler ved bruk over landegrensene.

Denne løsningen kan imidlertid ikke brukes sammen med GPS-data, og hindrer at myndigheter kan samle inn dataene. Franske myndigheter er skeptiske til å overlate teknologivalg til store, kommersielle aktører med betydelig egeninteresse.

Det europeiske personvernrådet mener at både sentralisert og desentralisert lagring kan være forsvarlige

alternativer, men at desentraliserte løsninger er best for dataminimering.

Ekspertgruppen som har evaluert Smittstopp, anbefaler å vurdere en mer desentralisert løsning når utprøvingsperioden er over. Dette vil kunne være mindre inngripende i personvernet, noe som kan øke utbredelsen av appen.

Lukket eller åpen kildekode?

I utviklingsmiljøer er det ikke uvanlig at kilde-koden publiseres åpent. På den måten vil flere øyne kunne vurdere ulike forhold, forbedre koden og eventuelt avsløre sikkerhetshull.

På den andre siden blottstilles svakheter og sikkerhetshull som kan utnyttes av de som ikke har gode hensikter. FHI har valgt lukket kildekode for Smittestopp-appen med henvisning til sikkerhetsrisiko og faren for misbruk dersom koden kommer i feil hender.

Det er en uenighet i fagmiljøene om dette er den rette strategien. Det europeiske personvernrådet anbefaler at kildekoden er åpen for en bredest mulig granskning fra forskersamfunnet.

Helse- og omsorgsdepartementet har gitt en ekspertgruppe tilgang til kildekoden for å vurdere personvern, sikkerhet og eventuelle sårbarheter. Ekspertgruppen anbefaler at så mye som mulig av kildekoden tilgjengeliggjøres som åpen kildekode, slik at brukerne får reell og direkte innsikt i hvordan deres data behandles.

Forfattere: Tore Tennøe og Hilde Lovett
Publisert: Juni 2020
Kontakt: post@teknologiradet.no / www.teknologiradet.no

Teknologirådet gir råd til Stortinget og regjeringen om ny teknologi
Dokumentet med kilder finnes på www.teknologiradet.no