Rådet for Digital Sikkerhed

26. marts 2020

Rådet for Digital Sikkerheds positionspapir for corona-virus og beskyttelse af personoplysninger

I forbindelse med Covid-19 har der i flere lande været brugt private telefondata til at opspore coronasmittede og dermed afdække, hvem de har været i kontakt med.

Overordnet mener Rådet for Digital Sikkerhed, at det er vigtigt, at der ses på mange forskellige muligheder for at bekæmpe corona – herunder også at se på om aggregerede, anonymiserede data kan bringes i spil for at vurdere om eksisterende policy tiltag virker, og få ideer til hvor man kan supplere indsatsen. Rådet for Digital sikkerhed mener samtidig, at man skal være varsom med at anvende telefondata på individniveau.

Indgrebet i en fundamental frihedsrettighed, privatlivets fred, bør således afvejes proportionalt med den effekt, man kan opnå med andre tiltag. Rådet for Digital Sikkerhed finder, at anvendelse af data er rimeligt i forhold til at få samfundet gennem en svær krise. Men med etablering af et system til overvågning af borgerne på individniveau via teleoplysningerne frygter Rådet dog, at et sådant system ved flere og flere lejligheder kan blive anvendt til at spore borgerne i forskellige situationer. Derfor finder Rådet, at der ikke bør anvendes telefondata på individniveau, men kun på aggregeret niveau. Som med anden Corona-lovgivning og tiltag bør der etableres solnedgangs-klausuler omkring brugen af tiltagene.

Samtidig er mange danskere i forbindelsen med Coronapandemien på Facebook blevet opfordret til at dele oplysninger om diagnoser og sygdomshistorik. Rådet for Digital Sikkerhed mener, at man skal være meget påpasselig med at dele den slags informationer. Når oplysningerne først er offentliggjort, kan disse opsamles og analyseres af hvem som helst – også af it-kriminelle til ondsindede formål som at stjæle brugernes identitet. Ligesom den platform du deler indholdet med kan f.eks. have rettigheder til at sælge dit indhold videre.

Corona-virus og beskyttelse af personoplysninger

Danmark – som resten af verden – står overfor omvæltninger, som ikke er set i nyere tid som følge af CoVid19 udbruddet. I Rådet for Digital Sikkerhed følger vi udviklingen tæt, og rådgiver løbende omkring det digitales rolle og ansvar før, under og efter krisen.

I nærværende holdningspapir drøfter vi konsekvenserne af forskellige tiltag som myndigheder og private har iværksat for at dele viden og få epidemiologisk viden om smittens færden og opførsel.

Der er for tiden en række tiltag i gang om at benytte personoplysninger om corona-virus til at skabe klarhed over virussens udbredelse: Statens Serum Institut har bedt om at indhente lokationsoplysninger hos teleselskaberne og kortlægge danskernes færden med det formål at få kortlagt om forbuddet mod forsamling opfyldes[1]. Både en række private[2] og en offentlig tjeneste beder om rapportering af data om

[1] https://www.dr.dk/nyheder/indland/coronavirus-seruminstitut-vil-tjekke-danskernes-bevaegelser-med-mobildata
[2] https://www.coronapp.dk/

Coronavirus. På Facebook findes også flere grupper, der adresserer corona-virus – herunder en der adresser danske forhold[3].

De retlige overvejelser

For det første kan der findes retligt grundlag for behandling af almindelige og følsomme oplysninger for offentlige myndigheder i databeskyttelsesforordningens[4] artikel 9 og 6. Private arbejdsgivere kan også finde et retligt grundlag for behandling af følsomme oplysninger, når de gælder folkesundhed jf. artikel 9 og medarbejdernes vitale interesser jf. artikel 6 og præambelbetragtning 46 når det gælder epidemier. Dette understøttes af udtalelser fra Det Europæiske Databeskyttelsesråd (EDPB)[5].

For det andet ville Folketinget kunne lave national lovgivning i medfør af databeskyttelsesforordningen artikel 23 for at sikre retligt grundlag for behandling. Hermed kan Folketinget samtidig sætte de grundlæggende principper i artikel 5 og de registreredes rettigheder i artiklerne 12-22 ud af kraft.

Der er med andre ord allerede ret vide rammer for at behandle personoplysninger om corona-situationen og Folketinget kan evt. udvide disse rammer.

- *Som med anden Corona-lovgivning og tiltag bør der etableres solnedgangs-klausuler omkring brugen af tiltagene.*

Deling af sundhedsoplysninger på sociale medier og via apps

Det står enhver frit for om man ønsker at offentliggøre sine personoplysninger – herunder følsomme personoplysninger som diagnoser og sygdomshistorik på f.eks. sociale medier. Når oplysningerne først er offentliggjort åbner de persondataretlige regler imidlertid op for, at de kan benyttes til andre saglige formål. Noget der umiddelbart kan fremstå som et individuelt bidrag til en god fælles sag fx at skabe et overblik over mørketallet af coronasmittede kan få andre konsekvenser.

Hvis man f.eks. deler helbredsoplysninger via Facebook, kan disse oplysninger opsamles og analyseres af hvem som helst – herunder personer der i realiteten vil den registrerede eller det danske samfund ondt. F.eks. kunne man opsamle oplysninger afgivet i en Facebook-gruppe og bruge dem til at sende en phishning henvendelse med det formål at stjæle brugernes identitet eller kryptere deres udstyr med ransomware.

Videre skal man være opmærksom på, at data eventuelt ikke slettes fra tjenesten, når corona-krisen er overstået, og desuden kan data opsamles til senere brug til andre ondsindede formål. Kort sagt aner man ikke, hvad de følsomme oplysninger kan blive brugt til, når først man har offentliggjort dem.

Der arbejdes verden over også på at lave forskellige private apps, som kan registrere corona-tilfælde, og hvortil man kan afgive helbredsoplysninger. Afhængig af hvem der står bag disse apps, er det også her tvivlsomt, hvad der videre sker med de oplysninger man giver fra sig.

- *Rådet for Digital Sikkerhed fraråder, at man deler følsomme personoplysninger på sociale medier eller til andre private tjenester. Hvis man alligevel ønsker det, anbefaler Rådet, at man laver sin egen*

[3] https://www.facebook.com/groups/198145384954774/
[4] https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:32016R0679&from=EN
[5] https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_2020_processingpersonaldataandcovid-19_en.pdf

lille risikovurdering og overvejer konsekvenserne ved at dele sine følsomme oplysninger med disse medier og tjenester. Der er en risiko for, at man mister kontrollen med de personoplysninger, man offentliggør ligesom de kan opsamles til senere brug til andre ondsindede formål. Endelig kan den platform, du deler indholdet med, f.eks. have rettigheder til at sælge dit indhold videre.

Rådet for Digital Sikkerheds holdning til myndighedernes tiltag

På den ene side åbner lovgivning som nævnt indledningsvist op for, at det er muligt for den offentlige sektor at gå langt indenfor de persondataretlige regler, når folkesundheden er på spil. På den anden side er borgerne sikret en fundamental ret til beskyttelse af deres privatliv, som kun meget sjældent skal tilsidesættes jf. Den Europæiske Menneskerettighedserklæring, Grundloven, Databeskyttelsesforordningen m.v.

Det er centralt i den forbindelse at vurdere om et forslag, som er et indgreb i den fundamentale frihedsrettighed, privatlivets fred, kan siges at være proportionalt i forhold til hvilket formål, der skal forfølges[6]. Kan man f.eks. opnå sit formål med mindre indgribende midler?

I en række lande har man fundet, at det var et proportionalt tiltag via teleoplysninger at spore individuelle borgere, der havde været sammen med smittede borgere, og efterfølgende mere eller mindre frivilligt sætte dem i karantæne[7].

- *Rådet for Digital Sikkerhed finder, at sporing af individuelle borgere med det formål at tvinge dem i karantæne ikke er proportionalt i et demokratisk samfund især henset til, hvor stor effekt man kan opnå ved nogle af de andre tiltag, der er iværksat.*

Man kunne forestille sig at teleoplysningerne i stedet blev anvendt på et mere overordnet niveau[8], hvor man f.eks. bruger data til at identificere forsamlinger af personer på afgrænsede geografiske steder (med det formål at evaluere om forbuddet mod forsamlinger virkede, herunder f.eks. i realtid og fastslå om mere end 100 mennesker er spontant samlet), identificere en øget rejseaktivitet mellem landsdelene (med det formål at se om befolkningen drager på påskeferie) eller identificere om visse typer af butikker har kunder (med det formål at identificere barer og storcentre, som ikke overholder pligten til at holde lukket).

- *Rådet for Digital Sikkerhed finder, at anvendelse af* fx aggregerede, anonymiserede *data ville være proportionalt. Der er i disse eksempler ikke mulighed for at forfølge den enkelte. Selv om data stammer fra individer, vil de i deres anvendelse være aggregerede og har dermed form af at være statistik.*

Rigspolitiet har i dag under visse omstændigheder mulighed for at spore borgerne via teleoplysningerne – f.eks. hvis der sker alvorlig kriminalitet et sted.

- *Hvis et mere generelt system til overvågning af borgerne på individniveau via teleoplysningerne først er etableret, frygter Rådet for Digital Sikkerhed, at et sådant system ved flere og flere lejligheder vil*

[6] https://politiken.dk/viden/Tech/art7725273/Seruminstituttet-afviser-at-svare-på-om-alle-danskere-skal-overvåges
[7] https://www.lbc.co.uk/news/coronavirus-residents-welded-inside-their-own-home/
[8] https://www.version2.dk/artikel/kampen-mod-corona-europaeiske-tele-operatoerer-leverer-lokationsdata-myndigheder-1090260

blive anvendt til at spore borgerne i forskellige situationer[9][10]. Dermed bliver det lettere fra politisk hold at sætte borgernes fundamentale rettigheder i form af retten til privatliv ud af kraft. Rådet vil også af den grund fraråde, at der etableres overvågning af borgerne på individniveau i tilknytning til coronakrisen.

[9] https://www.dr.dk/nyheder/penge/snowden-har-en-advarsel-til-danske-politikere-en-virus-er-skadelig-men-oedelaeggelsen
[10] https://www.ft.com/content/19d90308-6858-11ea-a3c9-1fe6fedcca75