

MAJ 2020

KONTAKTSPORINGSAPPS OG MENNESKERETTEN

I kampen mod covid-19 ønsker flere lande at gøre brug af 'kontaktsporings-apps'. Det gælder også Danmark, hvor en corona-app snart vil blive præsenteret. Men apps, der registrerer brugernes bevægelser og kontakter, rejser en række udfordringer i forhold til retten til privatliv og databeskyttelse.

Danmark er i færd med at udvikle en kontaktsporings-app, der skal supplere landets covid-19-strategi. Ideen er, at appen automatisk registrerer, hvem den enkelte borger har været i nærheden af, og giver besked, hvis telefonen har været tæt på en covid-19-smittet person.

En app som denne, der kan give et detaljeret overblik over borgernes kontaktmønster og helbredstilstand, vil kunne misbruges til overvågning af enkeltpersoner og grupper. Europarådet, Det Europæiske Databeskyttelsesråd, Europa-Kommissionen og Datatilsynet har således påpeget, at kontaktsporings-apps kan udgøre et stort indgreb i den enkelte borgers rettigheder. Det er derfor afgørende, at den udvikles med respekt for borgerens ret til privatliv og databeskyttelse.

MENNESKERETLIGE FORPLIGTELSER

Databeskyttelse er en del af retten til respekt for privatliv efter Den Europæiske Menneskerettighedskonventions artikel 8.

Samtidig sikres retten til beskyttelse af persondata også i EU's databeskyttelsesforordning og den danske databeskyttelseslov.

ANONYMITET ELLER PSEUDONYMITET

Databeskyttelse vedrører oplysninger om personer, og spørgsmålet om anonymisering eller pseudonymisering af data er derfor helt afgørende.

Anonyme oplysninger er oplysninger, der ikke kan føres tilbage til en person, og de falder derfor udenfor databeskyttelseslovgivningens område. Derimod er pseudonymiserede oplysninger omfattet af reglerne, idet oplysningerne kan kobles til personen ved brug af supplerende oplysninger.

Rent menneskeretligt er det derfor centralt, om oplysningerne indsamlet i app'en er uigenkaldeligt anonymiserede, idet der ellers gælder de krav til privatliv og databeskyttelse, der følger af menneskeretten og databeskyttelsesforordningen.

DECENTRAL ELLER CENTRAL KONTAKTSPORING

Kontaktsporing kan baseres på enten en decentral eller en central model.

Danmark vil anvende en decentral Bluetooth-baseret model med brug af software udviklet af Apple og Google.

I denne model registreres borgerens kontakt med andre ved hjælp af en tilfældig nøgle, der gemmes på telefonen. Hvis en person testes positiv for covid-19 og vil advare andre, uploader personen information om, hvor vedkommende har været de seneste 14 dage, til en statslig server. Andre telefoner kan løbende downloade information om smittede personer fra den statslige server, og appen sammenligner telefonens egne bevægelsesmønstre med de smittedes for at afgøre, om telefonen har været tæt på en smittet person.

Den centrale model adskiller sig ved, at udsøgning og notifikation af de telefoner, der har været tæt på en covid-19-smittet borger, sker centralt, og der overføres derfor flere oplysninger om den smittede borgers kontakter til staten.

FORMÅL OG PROPORTIONALITET

Det følger af menneskeretten, at tiltag, der begrænser borgernes rettigheder, kun må gennemføres, hvis et lovligt formål ikke kan gennemføres på mindre indgribende måder.

I forhold til den danske app er det imidlertid vanskeligt at vurdere proportionaliteten, idet hverken staten eller tekniske eksperter har kunne dokumentere, hvilken effekt en app vil have på smittesporing. Dette taler i sig selv for, at der stilles skærpede krav til, hvilke oplysninger der indsamles, og at formålet er klart afgrænset, ligesom der gælder krav om, at privatlivsbeskyttelsen er tænkt ind allerede i selve appens design og udformning

FRIVILLIGHED OG GENNEMSIGTIGHED

Den danske app er baseret på frivillighed og indebærer, at borgerne skal give samtykke til, at deres data samles ind og behandles. Det er imidlertid vigtigt at være opmærksom på, at samtykke ikke fritager fra de menneskeretlige forpligtelser, og at et fravalg af appen ikke må få negative konsekvenser for borgeren.

Som fremhævet af Datatilsynet skal det være tydeligt for borgerne, hvem der står bag dataindsamlingen, og hvad der sker med borgernes oplysninger. Gennemsigtighed er en forudsætning for, at man som borger kan beslutte sig for, om man vil bruge en corona-app og derigennem bidrage med sine oplysninger.