Bacheloroppgave

NTNU
Norges teknisk-naturvitenskapelige universitet
Det humanistiske fakultet

Victoria Orraya Tronvoll

Personvern og overvåkning ved bruk av digitale verktøy

En case analyse av smittestopp - appen

Bacheloroppgave i Medievitenskap
Veileder: Nina Lager Vestberg
Mai 2020

NTNU
Kunnskap for en bedre verden

Forord

Dette siste halvåret har vært både merkelig og bra. Motivasjonen har både vært opp og ned, og det har vært mye prøving og feiling før jeg kom i mål.

Jeg vil gjerne takke min veileder Nina, for å gi meg god veiledning, tips og råd til oppgaven. Familie og venner for støtten gjennom skriveperioden, spesielt min far som har fått meg til å yte mitt beste selv når motivasjonen ikke var på topp. Til slutt vil jeg takke mine medstudenter for å ha gjort studietiden til en av de beste årene av mitt liv.

Sammendrag

Det som presenteres i denne oppgaven, er hvordan vi som brukere av internett er blitt mer bevisst på vårt eget personvern, og hvordan Facebook håndterer personvern. Big Data, algoritmer og Data- mining er alle nye metoder å samle inn data på. Smittestopp – appen har vært en faktor som utfordret oss på for hvor langt vi ville la myndighetene få informasjon om oss da korona- pandemien brøt ut. Dette til tross for at vi etterlater oss spor på internett uansett. Spørsmålet som blir stilt i denne oppgaven omhandlet hvor vidt vi godtar at vi blir overvåket. Cambridge Analytica skandalen i 2018 viste hvordan reaksjonene ble rundt personvern og utviklet seg til å bevisstgjøre folk mer. Med bruk av nye digitale verktøy, blir det lettere å få en oversiktlig kartlegging av brukermønster til folk på internett.

Innholdsfortegnelse

1.Innledning

1.1 Problemstillingen

Hvordan kan vil tilpasse oss en verden fylt med digitale verktøy brukt av ulike aktører som alltid kommer til å vite hver minste ting vi gjør på nettet Er det viktigere å være bevisst på sitt ens eget personvern nå enn det var før?

Internettselskaper som Google, Amazon, Facebook og Apple er drevet av en tro på datateknologier som løsning på de fleste menneskelige problemer. Gjennom algoritmer, databaser og digitale nettverk skal verden kunne effektiviseres og forbedres (Enjolras, 2014, s. 85). Men når godtok vi at andre kunne bruke vår informasjon til sitt eget bruk? Personvern i dagliglivet og spesielt i sosiale medier har blitt mer visket ut. Hva skjer når millioner av brukeres informasjon blir delt på nettet uten samtykke? Den nye digitaliseringen former nye verktøy, som brukes til å fange ny digitalisert informasjon.

Da Facebook havnet i den omdiskuterte saken med Cambridge Analytica i 2018, ble det rettet stor oppmerksomhet på personvern og hvordan Facebook hadde solgt en stor mengde av privat informasjon til en tredjepart uten at brukerne var informert om dette. Nye Digitale verktøy, som «data- mining», Big Data og ulike algoritmer tas i bruk for å forbedre vår opplevelse på nettet. Ubevisst godtar vi dette når vi bruker de forskjellige tjenestene på nettet. Det har aldri vært viktigere å bry seg om hva man godtar og å være kritisk til informasjon som blir gitt på internett.

1.2 Valg av problemstilling

Jeg valgte å undersøke dette temaet nærmere på grunn av gjentakende hendelser der min personlig informasjon dukket opp flere steder på nettet uten å ha besøkt flere av nettsidene tidligere. Den type innhold som generes for oss på nettsidene og applikasjonene vi besøker, bruker oftest vår informasjon uten at det blir reist spørsmål om hvordan de får tak i denne informasjonen. Flere plattformer tar i bruk Big Data som informasjonskilde slik at de kan tilpasse innholdet sitt mest mulig mot hver enkelt bruker. Flere kan mene at en overvåkes når vi får tilpasset innhold, som vi tidligere har søkt på andre plattformer eller nettsider. Har vi som brukere rett på personvern i form av begrenset tilgang for tredjepart på slik informasjon? Eller må vi godta at enhver nettside bruker vår informasjon senere? Risikoen for uautoriserte tilgang, manipulering og stjeling av online – identiteter vil øke om store mengder privat informasjon blir lagt igjen på eller lekket til ulike nettsteder. Facebook har lenge vært likegyldig til personvern og er åpen om at innholdet er skreddersydd hver enkelt person basert på hva du liker og andre interesser på nettet.

1.3 Oppgavens oppbygging

Jeg vil først presentere teori relatert til de grunnleggende begrepene som vil nevnes jevnlig utover teksten, med tung vekt på hvordan Facebook operer i forhold til personvern. Deretter vil jeg gjøre en case analyse av Smittestopp – Appen og trekke ut hvorfor personvern var ett av de viktigste temaene i diskusjonen rundt Appen. Hvorfor fikk utviklerne en så stor mengde kritikk? Jeg kommer hovedsakelig til å bruke Cambridge Analytica skandalen som et eksempel på en hendelse, som gjorde verden mer oppmerksom på personvern, og skapte mistillit mellom brukerne og tjeneste - leverandørene. Oppgaven vil gi innsikt i hvordan digitale verktøy som Big Data, «data- mining» og algoritmer brukes av aktører for å kunne tilby det beste tilpassede innholdet til brukere av en tjeneste. Og hvor viktig er det å være kritisk til ens eget personvern og hvordan informasjon blir samlet om oss uten at vi selv er klar over det, uten at vi trenger å føle oss overvåket?

2.Teori

2.1 Nye Digitale verktøy

Når vi taster inn enkelte ord på Google vil det komme opp søkeforslag før du taster inn ditt hele søk. Selv om søket utføres er automatisk, er det brukerne bak det som er problemet, ikke selve søkene. Ta for eksempel algoritmer som er opplærte datagenereringer, som har som mål å finne et ønsket utfall best tilpasset individet. De brukes ikke bare til Google søk men også til en tredjepart som er interessert i søkehistorikken til hver person.

De fleste mobiltelefoner sporer brukernes lokasjoner med koblinger til et globalt posisjonerings- system. Facebook – og – Instagram- applikasjonene på telefonen samler også data om personen som bruker den. Dette er en systematisk overvåking og nøkkelen til dens makt er sammenheng. Eksempelvis kan Facebook korrigere en post der man har tagget venner tatt i Charlottesville, Virginia (Vaidhyanathan, 2018, s. 54). Det Facebook kan gjøre her er å genere bemerkelsesverdige nøyaktige antagelser om hyppigheten av møtene våre, hvordan forholdet er mellom oss, de neste felles bekjente, men også relativ inntekt og forbruker- vaner. Dette virker harmløst helt til en Facebook- bruker ønsker å misbruke denne informasjon for å skade til andre, eller at en undertrykkende statsmakt får kontroll på denne type informasjon. Grunnen til at Facebook gjør slike handlinger er for å genere innhold den tror vi trenger på nyhets- «feeden» vår. Roten til alt dette er et system av overvåkning ulikt det meste vi har sett i den vestlige verden. Og dette har nådd oss måter vi er uforberedt på å møte. Noen vil hevde at Facebook på mange måter utviklet seg til det mest gjennom- gripende overvåknings- systemet i verden. Samtidig hevdes det at det også er det mest uforsvarlige og uansvarlige overvåkningssystemet i den kommersielle verden (Vaidhyanathan, 2018, s. 55).

Hvordan er så vår utdanning og opplæringen til kritisk til bruk av Online tjenester? Her har ikke kjønn eller alder like mye å si som forskjellen i undervisning og opplæring, som er et mer permanent problem. Større bevissthet rundt algoritmer henger sammen med at brukerne har en høyere utdanning (Bucher, Booth & Gran, 2020). Uansett kan det være vanskelig å vite hvordan Internett fungerer i mange sammenhenger og hva som kan befinne seg av informasjon nettet.

2.2 Black box – en ukjent virkelighet

Begrepet «Black box» blir beskrevet av Taina Bucher, som et konsept som representerer alt det vi ikke kan vite. Opprinnelig ble den svarte boksen referert til en fysisk ekte boks, som inneholdt hemmelig krigsinformasjon under 2. verdenskrig. Det ble i senere tid en metafor for noe hemmelig eller det en er uvitende til (Bucher, 2019, s. 43). Algoritmer er ikke forskjellig fra det som er beskrevet om den svarte boksen. Det handler ikke bare om en mangel på kunnskap eller informasjon, men mangelen av ansvarlighet i bruken av og åpenhet rundt algoritmene. Viktige bedriftsaktører har enorme mengder kunnskap om vårt dagligliv, mens vi vet lite til eller ingenting om hvordan de bruker denne kunnskapen til å påvirke viktigheten av valgene vi eller de tar. Denne kunnskapen innebærer nye makt - konstellasjoner, ikke bare mellom aktører med informasjon om mennesker de overvåker, men også mellom aktørene imellom (Bucher, 2019, s. 45).

2.3 Big Data som et nytt begrep

Big Data er et ord, som i de nyere tider er blitt et moteord. Det er en samlebetegnelse for en stor mengde data - mer enn vanlig datakraft. Eksistensen av slike data kan reise nye problemstillinger av både teknisk, juridisk og etisk art (Enjolras, 2014, s. 81). Big Data innebærer faktiske registrerte handlinger, interaksjoner og transaksjoner individer og mellom individer og organisasjoner. Personvern er derfor viktig å forholde seg til, selv om det er vanskelig med tanke på hvordan sosiale medier kan viske ut grensen mellom personvern den personlige og den offentlige sfære. De nye teknologiske mulighetene som Big Data gir kan føre til misbruk av informasjon om hvert enkelt individ og true personvernet.

Det har lenge vært en potensiell utbetaling for sporing av blant annet objekter (forbrukere, innbyggere, kriminelle, brukere). Big Data er et relativt nytt verktøy for forskere og analytikere, og de understreker ofte virkeligheten av tilgjengeligheten av passende teknologier for å hente informasjon eller for «data mining». Dette innebærer bruk av enorme serverer, algoritmer designet for å raskt avsløre mønstre innen ellers meningsløse data, større bredbåndbredde samt høyere prosesserings- kapasitet (Vaidhyanathan, 2018, s. 65). En kan nesten føle seg overvåket av de nye datateknologiske verktøyene. Det fører til sporing av forskjellige individers handlinger og kommunikasjon på nettet. Big Data brukes også til det positive, og store web - baserte tjenester som Facebook eller Twitter lagrer kontinuerlig data til hver enkelt profil slik at tjenesten kan lettest mulig kan komme med såkalte venne - forslag.

Ved å ta i bruk nye digitale verktøy har vi mulighet til å oppdage problemer og upassende innhold som før gikk gjennom usett. Bilder som virker støtende blir undersøkt av Facebook- ansatte og lagret slik at det lages en egen unik signatur for hvert bilde. En algoritme som bruker kunstig intelligens kan skanne og matche bilder som blir lastet opp på Facebook. Bildet blir beholdt i en kort periode, før det originale bildet slettes, men samtidig beholdes det gjenværende «fingeravtrykket». Fingeravtrykket, som også kan være kjent som «hashing», tillater algoritmen til å matche det originale bildet med en endret eller et nytt bilde. Store teknologi- selskaper bruker lignende prosesser, som er en kombinasjon av menneskelig dømmekraft og algoritme screening (Vaidhyanathan, 2018, s. 75).

2.4 Data – Mining som en ny metode

«Data-Mining» - metoder, som er analyse av en enorm innholdsrik mengde med informasjon, som gjør det mulig å lage personlige brukerprofiler, som senere kan benyttes til å generere målrettet reklame, markedsføring eller produkter gjennom tilpassede «anbefalings- systemer». Det har derfor oppstått en ny nisje for såkalte informasjons – meglere, som selger informasjon om webtrafikk (i form av algoritmer, etc.), til både private og offentlige aktører (Enjolras, 2014. s, 82). Å samle inn slike meta- data på individnivå, gir Big Data mulighet til å samle inn og analysere omfattende og detaljert informasjon om en persons liv, aktiviteter, preferanser og ytringer. Digitale spor blir lagt igjen på ulike webtjenester eller apparater som er koblet opp til internett, som f.eks. medlemskort til ulike butikker, eller apparater koblet til Internett. Metadata som er knyttet til transaksjonsdata f.eks. e- post adresse eller IP – adresse, kan brukes til å koble ulike datakilder sammen og muliggjøre personlig identifikasjon (Enjolras, 2014. s, 86).

2.5 Trussel mot privatlivet

Data- Mining, maskinlærings- teknologi og Big Data kombinert, utgjør i økende grad en trussel mot ytringsfrihet og personvern. Regjeringer og private selskaper kan overvåke og analysere kommunikasjonen, som foregår privat på tvers av ulike brukerkontoer (f.eks. Google Gmail, Youtube, Chrome. Google+ etc.). Regulering av personlig informasjon, som er tilgjengelig digitalt, er i økende grad kontrollert av globale selskaper som er i privat eie (Facebook, Google, m.fl.), der brukerne har gitt fra seg rettighetene sine for å kunne benytte seg av tjenestene. Det er ikke bare Facebook hvor du må godta retningslinjene, som innebærer at en må gi ifra seg rettigheter. Det viser seg også at de fleste ikke leser nøye gjennom vilkårene til tjenestebruken, og er ikke klar over hva de samtykker til (Enjolras, 2014, s. 87). Personopplysninger skal i størst mulig grad være basert på innhentet samtykke fra den personen informasjonen blir hentet fra når en virksomhet skal behandle slik informasjon. Imidlertid tyder mye på at personvern vil bli mer visket ut i de nyere digitale media.

Personlig informasjon som blir gitt på forskjellige nettsider utgjør en stor verdi, og danner grunnlaget for reklameinntekter eller de kan bidra til å gjøre tjenester mer effektive og personalisert. Anbefalings- systemer blir derfor anvendt på store mengder av den personlige informasjonen individer har ute på nettet. Eksempelvis Google spør ofte om hvor du befinner deg når du skal søke opp noe på søkemotoren deres. Dette gir ikke bare et mer nøyaktig treff på hva de vil gi deg, men det gir også informasjon til algoritmene om hvor du er til neste søk.

Algoritmene vil altså huske hvor en person var til enhver tid, som gir dem muligheten til å kartlegge hver minste detalj om personen. Hva er det vi tror Big Data og algoritmer gjør? De samler informasjon om enkelt - individer og lagrer det. Algoritmene er til for å følge med på akkurat hva vi ser på. Dette reiser spørsmål om hvor stor makt de egentlig har over brukerne.

2.6 Facebook som overvåknings maskin

Alle som bærer rundt på et kamera festet til en mobiltelefon er agent for overvåkning. Slik som Susan Sontag (Vaidhyanathan, 2018) fortalte, lenge før Facebook og Instagram, så kaller kameraet på oss til å bruke det. Selv Sontag kunne ikke forestilt seg at milliarder av mennesker kom til å ha disse kameraene og at mange kunne komme til å misbruke dette. Men Facebook- gründeren Mark Zuckerberg kunne. Han bestemte at fotografi skulle bli nøkkelen til Facebook´s framtid. Hvert tilfelle av overvåkning blir til en del av et massivt bedriftsovervåknings- system med en gang bildet er lastet opp på Facebook eller Instagram (Instagram er eid av Facebook). Bildene er tagget med meta- data som avslører tid og lokasjon (Vaidhyanathan, 2018, s. 53). Folk tagger bilder med navn på andre mennesker på bildet, og avslører deres nærvær og bevegelser for andre. Kameraet i seg selv er knyttet til en enhet for konstant bedriftsovervåkning som ofte er plattformen de publiserer bildet på.

For dem som har vært aktiv på Facebook før 2014, og brukt spill som *Farmville, Mafia wars* eller *Word With Friends*, så eksporterte Facebook ikke bare betydelig informasjon om deres aktivitet, men også deres venners aktivitet. Facebook har derfor blitt sanksjonert av regjeringer rundt om i verden for deres praksis av samling, bruk og deling av personopplysninger uten full eller tydelig formidling og samtykke av de berørte. Men likevel fortsetter selskapet å misbruke sine brukere, men kan trøste seg av sin popularitet og kraft av tjenesten til å fortsette (Vaidhyanathan, 2018, s. 55).

Mark Zuckerberg mener derimot at all deling er god deling, og hvis mennesker delte mer ville verden også bli mer åpen og sammenkoblet, og dette er en bedre verden (Vaidhyanathan, 2018, s. 71). Dette var noe han riktig nok skrev i 2010 i *Washington Post,* og det utsagnet har drastisk blitt satt på prøve etter skandalen i 2018. Facebook har sakte men sikkert fått oss til å akseptere deres hoved- prinsipper og bli en bruker av et overvåkningssystem. Samtidig som Facebook mener de øker kontrollen brukere har over hva de velger å dele og med hvem. Som Zuckerberg også skrev i 2010, mente han at folk ikke ville ha fullstendig privatliv, og de vil ikke kunne ha noe hemmelig. De vil ha imidlertid ha kontroll over hva de deler og hva de ikke deler (Vaidhyanathan, 2018, s. 73). Zuckerberg har imidlertid bygget et system som beveger oss til å akseptere hans visjon av en bedre, koblet og sett verden.

3. Metode

Med tanke på tema har jeg valgt å gjøre en case analyse av smittestopp – appen som kom i 2020. Grunnen til dette er de dagsaktuelle diskusjonene som har oppstått rundt bruken av appen. Jeg kommer også til å trekke inn Cambridge Analytica skandalen i 2018 som inkluderte den mye brukte plattformen Facebook, et eksempel på en hendelse som gjorde flere bevisste på sitt eget personvern.

4.Analyse av Case

4.1 Smittestopp Appen

Overvåkning er ikke alltid lett å finne ut av, og ofte når vi nevner personvern blir George Orwells uttrykk «Storebror ser deg» nevnt. I de digitale tidene som har vært, kan det være vanskelig å oppdage hva det er viktig å være kritisk til. Da korona- krisen inntraff, ble det i samspill med Folkehelseinstituttet utviklet en applikasjon som skulle forhindre smitte ved å varsle ifra når brukeren nærmet seg enn smittet person. Når applikasjon ble

lansert gikk statsminister Erna Solberg ut og sa: «Vi kan alle være med på å stoppe smittespredning og redde liv. Hvis mange laster ned appen Smittestopp, kan vi åpne samfunnet mer opp og få friheten vår tilbake» (Aalen, 2020). Som Ida Aalen (2020) skriver i Aftenposten, er det mye som skal klaffe for at en smittstopp – app skal fungere som lovet.

Smittestopp- appen krever at man legger inn personlig informasjon for at den skal aktiveres. For at den i det hele tatt skal fungere, har utviklerne av appen anslått at rundt 60 prosent av befolkningen må ta den i bruk (Aalen, 2020). En må også ha en smart-telefon for at den kan lastes ned, samtidig som man må få med seg at den finnes i det hele tatt. Og selv om vi vet om den, må vi selv ville laste den ned. Selv om det er mange som er positive til det, kan det være vanskelig for enkeltpersoner som f.eks. de eldre, som ofte ikke benytter smart - telefon. Ifølge tall fra Kantars Interbuss (Aalen, 2020) – undersøkelse, er det bare en av ti som bruker applikasjonen på telefonen, som skaper problemer når det er et visst antall brukere som aktiveres for at applikasjonen skal komme til nytte. Etter at man har lastet ned appen, møter man en rekke innstillinger en må aktivere. Bluetooth, lokasjon og varslinger er noe som må skrus på for at den skal fungere. Helt til slutt må man registrere seg med telefonnummeret sitt, men til og med da støter man på tvilsomme lenker som kan få en til å undres. Etter å ha godtatt en lang personvernerklæring kommer man seg endelig til selve applikasjonen. Videre må det legges til at det kreves en smarttelefon med god nok batterikapasitet, dette på grunn av GPSen som opererer i bakgrunnen av appen, og nødvendigvis Bluetooth, som helst skal være aktivert under bruken av applikasjonen. Dette krever mye energi og tapper enhver mobiltelefon for strøm, som fører til at telefonen må lades ofte.

Om appen fungerer som den skal, vil den varsle brukeren om vedkommende har vært i nærheten av en smittet person i mer enn 15 minutter. Sånn sett er det en genial måte å kunne begrense smitten. Det negative er at den ikke varsler deg om hvem du har gått forbi, om du har brukt eventuelle bankterminaler eller dørhåndtak som kan være smittet, fordi du ikke har vært i nærhetene av dem mer enn 15 minutter. Uansett må en smittet person frivillig registrere dette i appen, og fysiske gjenstander vil naturlig nok ikke kunne varsle ar de er gjenstand for smitte. Men hva om en faktisk blir varslet om at du er nær en smittet, men at en ikke var nærme nok til å bli smittet? Vil det skape et press om at en burde teste seg og skape unødvendig bekymring, unødvendig testing og ekstra belastning av helsevesenet? Enda verre blir det om feil bruk skulle gi falske positive signaler. Uansett om det er relativt få som laster ned appen vil, som Folkehelseinstituttet fremhever, dataene likevel kunne brukes til forskning (Aalen, 2020). Imidlertid burde da appen kanskje blitt omdøpt til Smitteforskning framfor Smittestopp.

4. 2 Personvern

Selv om applikasjon er laget for å begrense og eventuelt stoppe smitte, og derfor framstår som samfunnsnyttig, er det personvern som er blitt hovedfokuset i mediene. Hilde Nagell (Aalen, 2020) skriver «Personvern trumfer ikke alt. Det må veies opp mot liv og helse». Et utsagn som kan kritiseres med tanke på hvordan gode hensikter før har blitt misbrukt i forhold til personvern. Spesielt rettet mot Cambridge Analytica hendelsen, der flere millioner Facebook - brukere og ikke brukere, ble misbrukt i forhold til informasjon om deres ytringer, og fikk en innvirkning på valget i USA. Hendelsen ble blåst opp til en stor sak og personvern ble ett ord, som i ettertid ble viktig for det de fleste brukere av internett. Cambridge Analytica (CA) er et selskap som ble etablert i 2013 for å gjøre «data- Mining», dataanalyse i forhold til velgernes holdninger og benytte informasjonen til å definere strategisk kommunikasjon for valgkampanjer. Senere benyttet de informasjonen om Facebook – brukere og solgte analyser av materialet. CA er et eksempel på et selskap som misbrukte persondata til tilfeldige Facebook - brukere (Granville, 2018). Når Facebook valgte å inkludere en tredjepart i tjenestene deres, skulle de ha informert brukene deres om det. Uten samtykke til dette fra brukerne, forverret saken mer. Mye av informasjonen hentet fra tredjeparten CA ble brukt til å utarbeide politiske kampanjer, der blant annet Donald Trump dro nytte av dette.

Å registrere folks bevegelser er et inngrep i den enkeltes privatliv og vil ikke bli akseptert i en normaltilstand (Dahl, 2020). Ett år etter at CA - skandalen brøt løs, var det fortsatt ingen av selskapene som hadde svart ordentlig for seg på spørsmålene rundt personvern og privat informasjon om selskaper og forbrukere, som ønsker at Internett skal fortsette å være fritt og praktisk, men også ha en viss kontroll på deling av informasjon. En kan

føle at man mister retten på seg selv når det blir klart hvordan privat informasjon blir gitt videre uten samtykke. Men kan man skylde på seg selv ettersom mange ikke leser nøye gjennom vilkårene når de tar i bruk en tjeneste (Enjolras, 2014, s. 87)? Det kan reise diskusjoner rundt hvorvidt man skal skylde på aktørene for å ikke opplyse nok. Derfor er det viktig at det blir gitt grundig informasjon om hva appen innebærer, men også informasjon om hva som kan skje hvis man velger å ikke laste den ned (Sævold, 2020).

Appen har ført til misnøye hos flere på grunn av mengden informasjon som kreves for at applikasjonen skal fungere. Flere finner det ubehagelig at myndighetene skal vite hvor en befinner seg til hver tid. Mange har nevnt ordet overvåkning, som kan gi assosiasjoner til Big Brother, som tidligere var en populær TV- serie. Flere kommenterer på hvordan det kan føles å være overvåket 24/7 (Rønsen, 2020). Helseminister Bent Høie kom med en uttalelse om at det ikke er snakk om overvåkning av enkeltperson men bare hvordan folket som «helhet» beveger seg, samt at all informasjon krypteres (Rønsen, 2020). Det er ikke løgn Høie kommer med, men det er vanskelig å tro at «ingen enkeltpersoner vil eller kan overvåkes». Den store utfordringen er knyttet til innsamlingen av posisjonene til brukerne (GPS), som sendes til store sentrale lagre, som er det Folkehelseinstituttet og Simula (utviklere av appen) har valgt å gjøre for Smittestopp i Norge (Skille & Gundersen, 2020).

4.3 Bekjempe pandemi med teknologi

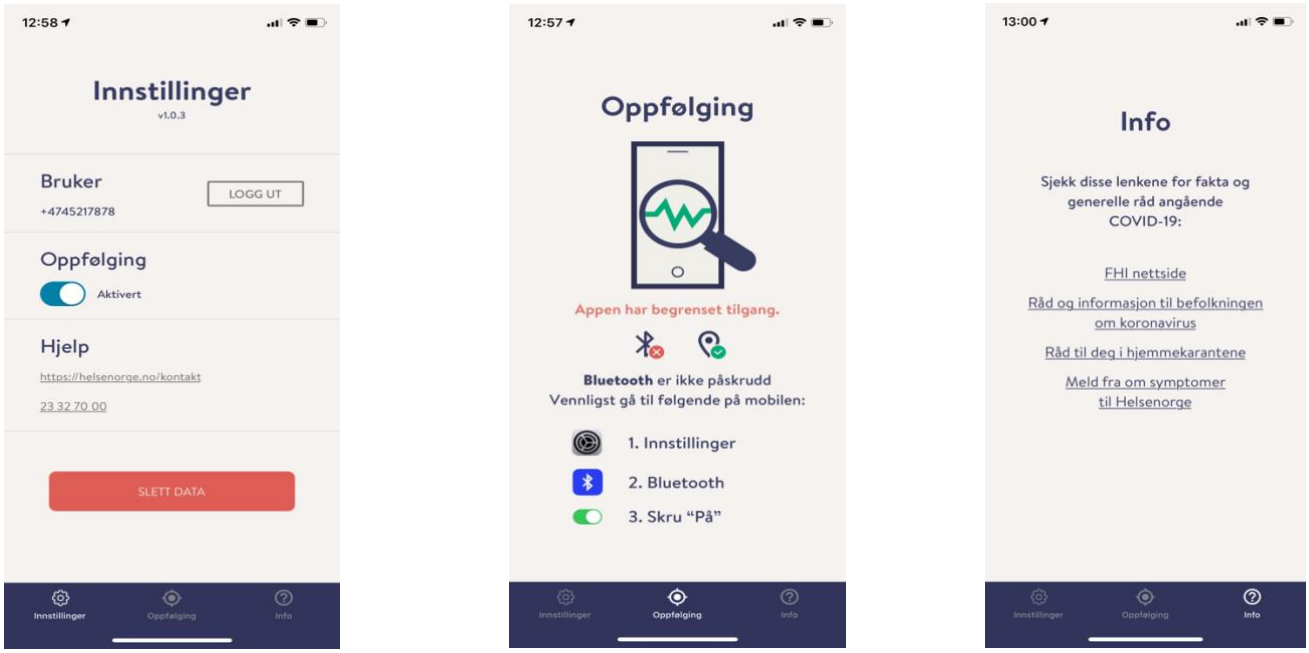
Å bruke moderne digital teknologi til å hindre en pandemi er akkurat den veien teknologien burde gå. Ved hjelp av lokasjonsdata fra både GPS og Bluetooth, som ikke er så nytt for mange, kan være med å hjelpe på å stanse smitten. Har man oppholdt seg med en smittet i mer enn 15 minutter får man SMS fra myndighetene med pålegg om karantene. Men ingen er i stand til å sikkert sjekke om en faktisk setter deg selv i karantene. Samtidig som myndighetene mener vi må ha tiltro til appen må de også ha tiltro til at brukerne følger restriksjonene som blir gitt av myndighetene. Kyrre Lekve (Sævold, 2020) uttaler at appen ikke vil spore dem som er i hjemme karantene. Det er teknisk mulig, men det vil ikke bli gjort. Den norske befolkningen ville aldri godtatt at politiet eventuelt skulle gått inn og håndhevet karantene på den måten. Apper benyttet i enkelte land i Asia gjør nettopp dette, og det er også veldig effektivt. Imidlertid er det antagelig få i Norge som ønsker overvåkning på det nivået. Det kan skape mindre tillit til myndighetene, noe som er nøkkelen til at applikasjonen kan ha en positiv effekt. Vi trenger en felles digital innsats mot viruset. For at dette skal skje kreves det tillit.

Datatilsynet er positive til hvordan folkehelseinstituttet har valgt bruke applikasjoner og annen type teknologi for å bekjempe pandemien. Uansett understreker de at personverninngripende tiltak må være «nødvendige, egnede og forholdsmessige» (Dahl, 2020). Det foregår i flere land utvikling av apper, som kan spore og varsle personer som er smittet med korona viruset. Det europeiske *personvernrådet* har gitt innspill om viktigheten av tillit, og hvordan appen må bygge på frivillighet. De kommer også med en interessant kommentar om at det burde gis informasjon om at alle data skal slettes eller anonymiseres etter at pandemien er over (Dahl, 2020). De fleste har tillit til myndighetene og at de kan samle informasjon til smittevern – i hvert fall når det står liv på spill. Men det er uansett store utfordringer ved å samle inn helse - og persondata. Det er alltid en risiko for at data med sensitive opplysninger kan havne i gale hender gjennom lekkasjer, hacking eller menneskelig feil. Og når informasjonen fra appen skal lagres i en stor sentral database, kan det få store konsekvenser dersom feil personer får tak i den informasjonen (Halsen, 2020).

Er vi mer villig til å gi fra oss personlig informasjon når det er anbefalt av myndighetene -spesielt når vi befinner oss i en pandemi, der det kan bety å redde liv ved å gi tilgang til hver minste bevegelse vi gjør? Den felles dugnaden, som Erna Solberg har oppfordret oss til - innebærer det å måtte gi slipp på personvernet og å laste ned Smittestoppappen - som en god borger? Selv om vi gjør det, må det tas i betraktning at det ikke bare er ungdommer som er godt vant med smarttelefoner, men også eldre mennesker, som må ta i bruk applikasjonen. Det er nettopp der det stopper. Slik som Ida Aalen (2020) i Aftenposten skriver så er det mye som må klaffe for at dette skal kunne fungere.

4. 4 Brukervennlighet

Designet til appen er ikke vanskelig satt sammen, og man kan se hvordan designet er satt sammen på en brukervennlig måte som skjermdump i figur 1 viser. Varslingen om man har vært sammen med en smittet blir formidlet via SMS – melding. Dette fordrer selvfølgelig at den man er sammen



Figur 1. Skjermdump fra Smittestopp – app, lastet ned [26.april] via iOS.

med benytter appen og opplyser at man er smittet. Trykker man på appen vil man få opp tre kategorier en kan velge - innstilling, oppfølging og info. Under oppfølging vil en kunne se om tjenesten er aktivert, og hvis ikke står det instrukser en må følge for å aktivere appen. Slik som vi kan se på under ´Oppfølging´ i appen (andre bilde i Figur 1), står det tydelig at det er begrenset med tilgang. Vi ser at det tydelig er en veiledning fram til hvordan man skrur på det som mangler for å fullt aktivere appen. Dette gjør det enklere for uerfarne å navigere seg fram. Under info er det en mengde med lenker en kan trykke på, som sender en videre til Folkehelseinstituttets nettsider.

Men hvem er det som legger inn i appen at en er smittet? Det har ikke kommet nok informasjon rundt hvordan eller hvem, som vet at en er smittet? Enhver kan gå lenge uten å bli testet og være smittet uten å vite det. En kan ikke selv taste inn om en tror en er smittet eller føler symptomer på det, bare om en beviselig er smittet. En er derfor avhengig av resultater av en test. Dette kan ha både positive og negative sider. På info-kategorien er det en rekke lenker en kan trykke på, som omhandler forskjellige temaer relatert til viruset. Der kan en blant annet melde inn om symptomer til Helse Norge. Tilgjengeligheten appen har for at brukere kan ta kontakt om det er noe man lurer på er en positiv merverdi. Uansett om en melder fra om symptomer vil ikke det kunne vises i appen. Gir da applikasjonen en falsk trygghet med å få folk til å tro at man alltid er sikker hvor enn man går gitt at appen ikke varsler om eksponering mot smittet person? Videre kan en spørre seg om det da er fritt fram for smittede å ferdes i det offentlige rom. Pålagt isolasjon og karantene skulle vel nettopp sørge for å unngå eksponering mot smittede, og slik sett er vel appen ikke nødvendig?

4.5 «Big – Data» om ditt personlig liv

Myndighetene sitter på er en stor mengde data om Norges befolkning, «Big Data» som inneholder en stor mengde opplysninger om hver enkelt person. Datatilsynet mener her at det burde gis en tydelig og fullstendig

informasjon om hvilke opplysninger som samles inn, og hvilke formål dataene skal brukes til. I tillegg bør det opplyses om lagringstid (Sævold, 2020). «Data- Mining» utgjør en trussel mot ytringsfriheten ved at det samles inn store mengder data, som via analyse generer ny informasjon om befolkningen. Deretter kan en selge de informasjonen som samles inn om individene til en tredjepart (Enjolras, 2014, s. 82). Analytikere finner et mønster av rå- data, som kartlegger hva vi eksempelvis søker opp på Internett og derfor er mest interessert i. Dette er mange av oss klar over når vi får opp innhold som er målrettet oss, men det vi ikke vet er hvor ulovlig det er å selge den type informasjon til bruk for en tredjepart. Det ble derfor ekstra problematisk når Cambridge Analytics gjorde nettopp dette. Smittestopp appen kan ikke direkte sammenlignes med hendelsen som skjedde tilbake i 2018, men det er et tema som er relevant.

Det er ingen hemmelighet at smittestopp - appen kan sitte med mye informasjon hvis den brukes aktivt. Men før en laster ned, vil det komme tydelig fram at FHI ikke misbruker data de samler inn til å sjekke om brukeren overholder råd og pålegg fra myndighetene. Alle innsamlede data og personlig informasjon vil automatisk bli slettet etter 30 dager, samtidig som det er mulig å slette egne data når man er inne på appen. Dette gjør det vanskelig å kritisere misbruk av eventuelle data, når det står klart i retningslinjene hva som skjer med dataen etter en gitt periode.

Selskaper slik som Google og Facebook bruker Big Data samlinger og analyser, dette er hjertet av deres inntektsbringende funksjoner (Vaidhyanathan, 2018, s. 69). Dette blir beskrevet som forbedringer av «brukeropplevelse». Linjen mellom stat og kommersiell overvåkning, betyr forså vidt ingenting. Data innsamlet av en institusjon er enkelt overført og hentet ut, brukt og misbrukt av en tredjepart. Eksempelvis kan et selskap kjøpe forbruker- data fra et supermarked, og deretter selger denne informasjonen videre til epost - markeder, politiske partier, eller til og med til lokale retts - instanser. Data kan og samles fra statlige instanser som stemme registreringer, gjerninger, bil merker, med mer og selger det til direkte- marketing firmaer som tar nytte av dette. Det er imidlertid få som har lyst til å fraråde bruken av Big Data. Dette kan ha sammenheng med at det tilbyr klare fordeler for det offentlige. Vi må imidlertid fortsatt forstå de sosiale «kostnadene» like mye som fordelene, og ikke tillate at den raske fremveksten av nye teknologiske muligheter hindrer oss i å ha en kritisk holdning til nye informasjons- teknologier. Den politiske diskusjonen av teknologiens bruk og misbruk må derfor ivaretas (Vaidhyanathan, 2018. s, 66). Eksempelvis vil lett tilgang til data muliggjøre raskere og bredere epidemiologiske vurderinger og analyse av virkning av ulike tiltak i en krisesituasjon som samfunnet er inne igjennom korona–epidemien. Det ville derfor uhensiktsmessig å suspendere Big data som et teknologisk system i praksis.

4.6 Personvernforordningen

Norge vedtok i 2018 en ny personopplysningslov som inneholdt EU´s personvernforordning (GDPR). Det setter retningslinjer for innsamlingen og bruken av personlig informasjon til de som lever i EU (Blaker, 2018). Dette førte til at mange forbrukere fikk flere rettigheter når de brukte en tjeneste til en virksomhet, de har ikke lov til å til å behandle personopplysninger med mindre et samtykke ble gitt fra den det gjeldte. Smittevern- appen har derfor funksjon der du kan slette informasjonen om allerede brukt data, som befinner seg i appen. Hvorfor har applikasjonen fortsatt fått så mye kritikk selv om det står mye info om appen på Personvernerklæringen? Det synes tydelig relatert til holdningen rundt det å dele informasjonen sin på en bevisst måte. Folk flest synes å være mer skeptisk når man er bevisst på at en blir overvåket. Det kan jo diskuteres om man burde være mer mottakelig for å dele informasjon når det handler om en felles smitte-dugnad i landet. En nyere holdning til mediene, spesielt etter Facebook´s store skandale som omhandlet personvern til brukerne, synes å ha oppstått. Det viser hva som kan skje når informasjon havner hos uvedkommende fra det man trodde var en sikker applikasjon og hadde som de fleste hadde såpass god tillitt til.

4. 7 Tillit

Hovedgrunnen til at mange ikke vil laste ned appen ligger sannsynligvis i at de ikke tror den vil fungere. Den yngre generasjonen igjen er mer opptatt av sitt eget personvern og av mulig overvåking, mens de eldre bekymrer seg mer for nytten av appen, og om den er nødvendig å laste ned? Fungerer den? Men om det skal sies varsler

den bare om du har vært nær den personen i mer enn 15 minutter. Dette synes å gi en usikker måte å kartlegge om en har vært eksponert mot en smittet person. Enda verre hadde det jo selvfølgelig vært om det var et kart med oversikt over de smittede i området en befinner seg, selv om det ville vært den mest effektive løsningen for å se hvem som var smittet, og dermed unngå disse personene. Dette hadde trolig vært et betydelig brudd på personvernet, og de fleste ville neppe ha gått med på det. Hele tiden etterlater vi lange digitale spor hver dag, men nå har vi muligheten til å bruke data om oss til å forhindre og kartlegge smittespredning (Sævold, 2020).

De fleste nettsider vil vite hvor en befinner seg for å kunne gi en best mulig søkemulighet for vedkommende. Applikasjonen Tinder fungerer ikke uten at stedstjenesten er skrudd på, og vil alltid være på i bakgrunnen når en benytter mobiletelefon. Facebook og Instagram kommer som regel opp med forslag om hvilket sted du vil tagge på statusen eller bildet ditt. Hvordan unge menneskers rykte i varierte kontekster behandles har vært et samtaleemne i mange dårlige gjennomførte debatter i tidligere år. Personvern, betyr like mye som enhver sosial norm, lover eller teknologier. Men skal vi anta at «personvern er død» fordi unge mennesker ser ut til å dele all slags av detaljer gjennom sosiale medier (Vaidhyanathan, 2018, s. 71)? Grunnen til at vi plutselig er blitt så oppmerksom på vårt eget personvern, kan stamme tilbake til Cambridge Analytica-episoden.

4. 8 Overvåking

I Norge er ikke overvåking noe vi normalt har trengt å bekymre oss over. Gun Peggy Knudsen (Skille & Gundersen, 2020) sier til NRK at Smittestopp er utviklet for norske forhold, og at den baserer seg på tillit mellom borgere og stat i Norge. Bakgrunnen for dette er de svært inngripende tiltakene vi har i samfunnet i dag, der appen er ett av flere tiltak som kan være med å håndtere krisen (Skille & Gundersen, 2020). Selv om Folkehelseinstituttet går ut og sier at appen alene ikke er noe som vil kunne legitimere overvåkning av andre (Skille & Gundersen, 2020), er det uansett grunn til å være kritisk til at slike applikasjoner publiseres. Hvis vi skulle få en global aksept for at slike apper er godtatt vil det bli vanskelig å forby dem igjen senere (Skille & Gundersen, 2020). Ved å fortelle oss selv at vår app er OK, skaper det allerede en implisitt aksept for at Norge skal kunne bruke en slik løsning ved en senere anledning. Selv om det er første gang Norge godtar at en slik app laget av Norske utviklere blir brukt, er det flere utenlandske applikasjoner vi godtar i hverdagslivet vårt uten at vi tenker så nøye gjennom retningslinjene de opererer med.

Selv om det blir fortalt at brukere ikke vil bli overvåket fra produsentene bak Smittestopp – appen, er det fortsatt en fin grense mellom hva som kan klassifiseres som overvåking og ikke. Appen er klar på at den trenger både Bluetooth og lokasjonsdata for at den skal kunne brukes. Det vil dermed være en form for overvåking for hvert steg du tar når du bruker appen.

4.9 Vi lever i en delings – verden

Den nye digitale verdenen fortsetter å utvikle seg, samtidig som nyere digitale verktøy vil bli laget. Alt vi kan gjøre er å utvikle oss i takt, som innebærer å lære oss ny kunnskap. Fram til nå har vi startet å sette oss inn i nåtidens nye digitale verktøy, som algoritmer og Big Data. Før var kunnskapen forbeholdt dataingeniører eller de spesielt interesserte. Holdningen vår til de digitale verktøyene trenger nødvendigvis ikke å bygges på tillit, men aksept om at de vil befinne seg sammen med oss når vi er på nettet. Istedenfor å kritisere verktøyene, er det aktørene bak som man burde være skeptisk mot.

Teorier grunnlagt på en bundet liberal individualisme mislykkes stadig på å regne ut hvordan vi lever våre liv i en nettverks-verden. Tross alt lever ingen av oss totalt isolerte liv. Vi er en del av et sosialt og kulturelt mangfold. Vi lager og utvikler oss dynamisk som i tid samtidig sammen med andre, og våre interesser og sympatier forandres. Vi kan se at personvern ikke bare gjelder informasjon om oss selv. Grensene endres stadig, og kontekster blandes (Vaidhyanathan, 2018, s. 64). Å forby bruken av de digitale verktøyene ville vært en tvilsom vei å gå og ville vært å ta et steg tilbake i den digitale utviklingen.

5. Konklusjon

De fleste av oss vil eie en mobiltelefon i overskuelig framtid. Det kan gjøre det vanskelig å ha en kritisk holdning til hvor stor grad vi vil være villig til å dele opplysninger om oss selv, noe som i verste fall betyr at vi kan overvåkes av en tredjepart. Så lenge vi tar i bruk mobiltelefonen vår, vil det som regel innebære en form for overvåking. Den generelle «overvåkningen» som foregår overalt i samfunnet blir oftest oversett av oss brukere. Apper sporer mobil – og internett – brukerne uten at bekymrer oss nevneverdig. Kanskje kan det være fordi vi alle i stor grad gjør det samme og benytter de samme tjenestene, som gir en generell aksept? Vi har dermed levet med en viss sporing av eller overvåking av våre handlinger på Internett uten at det har vært opplevd som et stort problem. Cambridge Analytica - saken i 2018 gjorde imidlertid at personvern kom i søkelyset, og gjorde befolkningen bevisst på hvordan Facebook opererte med person- informasjonen vår. Saken viste også hvordan andre tjenester bruker en stor mengde informasjon om oss.

Begrepet «Black Box» har hatt og vil fortsette å ha en betydning fremover, ettersom det fortsatt er en stor uvitenhet rundt temaet Big Data og de nye digitale verktøyene som bl.a. algoritmer og «data- Mining». Privatlivet vårt, som de fleste alltid vil holde for seg selv, vil bli mer eksponert i takt med utviklingen av nye tjenester. Smittestopp appen er et eksempel på en tjeneste, som ble utviklet i et tidsrom der den til en viss grad var nødvendig, men der det ikke ble gitt nok informasjon rundt applikasjonen. Dette førte til skepsis rundt bruken av den. Det vi kan gjøre fremover er å anbefale gode internett – applikasjoner, og å hjelpe både eldre og yngre mennesker til å tilegne seg nødvendigvis ikke mye, men litt kunnskap om hvilke valg man kan velge å bør ta på nettet. Med mindre vi velger å avstå fra et digitalisert samfunn, noe som for de fleste er nærmest utenkelig, er det vanskelig å unngå eksponering mot det som skjer på Internettet. Dette betyr at vi vil legge igjen digitale spor etter oss selv. Så lenge vi har mobiltelefonen i baklommen vil vi alltid «forfølges» av leverandører på Internett.

Referanseliste

Aalen, I. (2020, 19.april). Korona kan ikke bekjempes gjennom ukritisk teknologioptimisme. *Aftenposten, A magasinet.* Hentet fra https://www.aftenposten.no

Blaker, M. (2018, 19.mai). Hva er GDPR og hva betyr det for deg? *Nettavisen.* Hentet fra https://www.nettavisen.no

Bucher, T. (2018*). If...Then: algorithmic Power of Politics.* New York: Oxford University Press.

Dahl, J.S. (2020, 16. april). Vil kontrollere smittestopp. Hentet fra https://www.datatilsynet.no

Enjolras, B. (2014). Big Data og samfunnsforskning. *Nye muligheter og etiske utfordringer, 55*(5), 80-89. Hentet fra Https://idunn.no

Gran, A.B. Booth, P. & Bucher, T. (2020). To be or not to be algorith aware: a question of a new digital divide? *Informatiom, Communication & Society.* https://doi.org/10.1080/1369118X.2020.1736124

Granville, K. (2018, 19.mars). Facebook and Cambridge Analytica; What You Need To Know as Fallout Widens. *New York Times.* Hentet fra https://www.nytimes.com

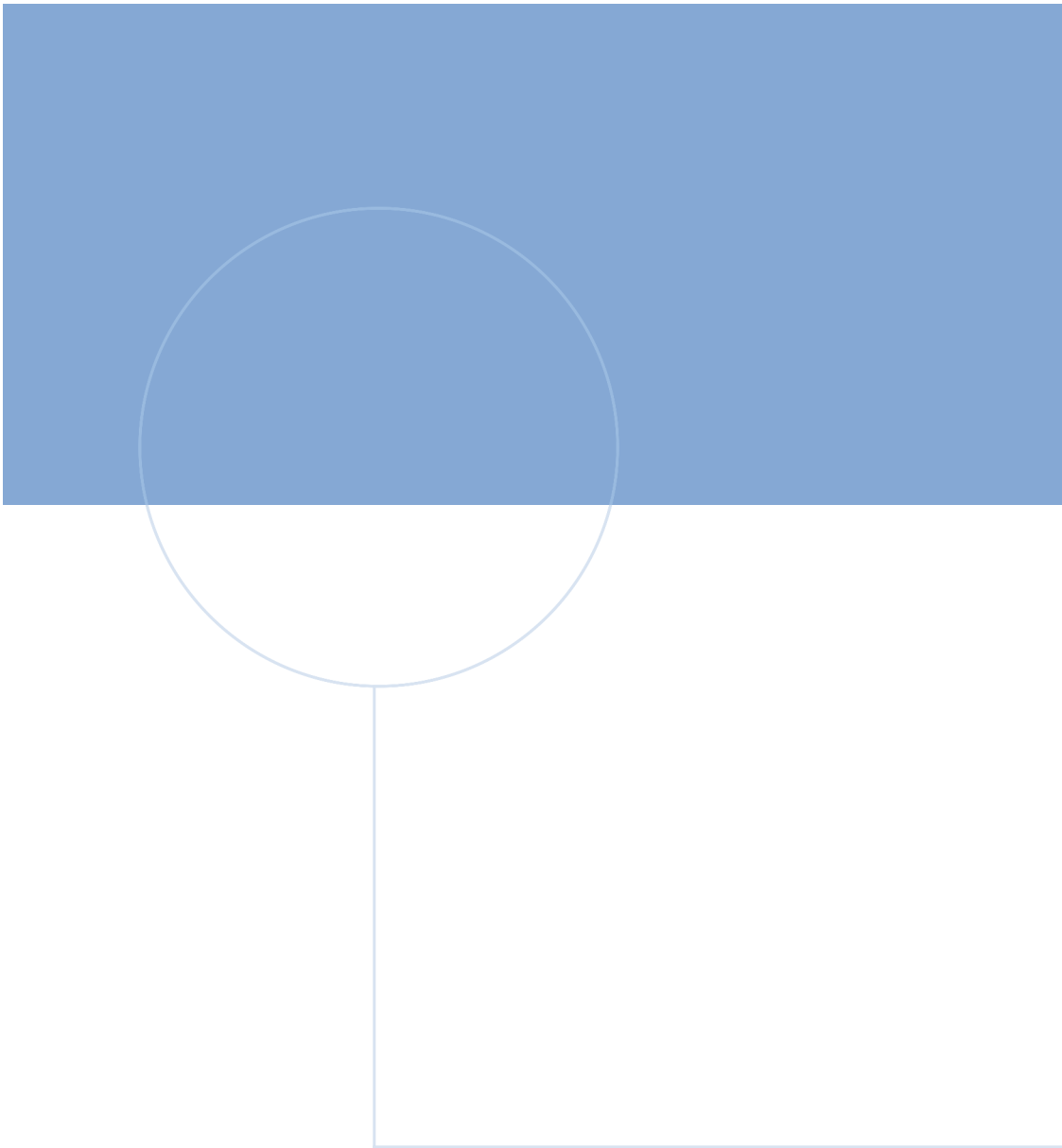
Halsen, F. (2020, 17.april). «25 under 25» om smittestopp appen: «folkehelseinstituttet ser deg». *VG.* Hentet fra https://www.vg.no

Rønsen, A. (2020, 17. april). Smittevern- app = Personovervåking? *Nettavisen.* Hentet fra https://www.nettavisen.no

Skille, Ø.b & Gundersen, M. (2020, 20.april). Hundrevis av it-eksperter fra hele verden ut mot sporingsapper som norsk smittestopp. Hentet fra https://www.nrk.no

Sævold, M. (2020, 30.mars). Bør du laste ned myndighetenes smittesporings-app? Dette sier Datatilsynet. Hentet fra https://www.digi.no

Vaidhyanathan, S. (2018). *Antisocial Media: How Facebook Disconnects Us and Undermines Democracy.* New York: Oxford University Press.



NTNU

Kunnskap for en bedre verden