Helseappens bevisverdi i en etterforskningsprosess

En empirisk oppgave

BACHELOROPPGAVE (BOPPG30)
Politihøgskolen
2021

Kand.nr: 110 og 111
Antall ord: 8683

SAMMENDRAG

I vår avsluttende oppgave på Politihøgskolen har vi valgt å gjøre en studie med følgende tematikk; «Hvilken bevisverdi kan digitale spor generert fra helseappen på smartenheter gi i en etterforskningsprosess?».

Gjennom en kvalitativ studie med intervju som fremgangsmåte har vi samlet inn data, og sammenlignet dataene opp mot teorien som finnes på temaet. I valget av informanter har vi sett etter ansatte med spesialkompetanse på feltet eller som kun jobber med digitale spor. Vi så på dette som relevant for den informasjonen vi ønsket å søke. Studien er tatt ut ifra syv informanter for å kunne ha et godt sammenligningsgrunnlag når vi skal se dette opp mot teorien.

Etter endt studie ser vi at tilgangen til- og behovet for digitale spor kommer til å øke, og dermed bør også prioriteringen av kompetanse og fagforståelse øke. Vi lever nå i en verden som stadig blir mer digitalisert, og det samme gjelder kriminaliteten. Det blir dermed viktig at det gjøres forskning og studier som ivaretar de nye digitale aspektene av politiarbeid, etterforskning og straffeforfølgelse.

Vi konkluderer med at data innsamlet ved hjelp av helseappen gir høy bevisverdi sammen med andre opplysninger i en straffesak, men gir lavere bevisverdi alene.

FORORD

Denne bacheloroppgaven er en avsluttende del av et tre-års studium ved Politihøgskolen. Vi har hatt tre innholdsrike, utfordrende og lærerike år, og setter stor pris på å kunne avslutte disse tre årene med et prosjekt som har fanget vår interesse. Arbeidet med oppgaven har gitt oss mulighet til å bruke kunnskap vi har opparbeidet oss gjennom disse tre årene, samt gjøre grundigere undersøkelser i et emne som interesserer oss.

Vi vil takke vår veileder Robert Furuhaug som har gitt oss utrolig god veiledning, i alt fra hvilke informanter vi kan kontakte til digital kunnskap om temaet vi har valgt oss. Vi vil også takke Politihøgskolen for tre fantastiske år.

I tillegg vil vi takke alle informanter som stilte opp til vårt bachelorprosjekt. Vi setter stor pris på all hjelp vi har fått, åpenhet og et genuint ønske om å bidra til oppgaven. Det er grunnet informantene at vi har hatt muligheten til å gjennomføre dette.

Sist vil vi takke både familie og nære venner for hjelpen og støtten de har gitt oss i løpet av både denne perioden, og hele studiet. Det har betydd mye for oss begge.

Politihøgskolen, april 2021.

INNHOLDSFORTEGNELSE

1.0 INNLEDNING

Hva er digitale spor og hva har det å si for etterforskningsprosessen? Samfunnet er i stadig endring og blir stadig mer digitalisert. Økt kunnskap om digitale spor og den digitale endringen som skjer i samfunnet blir stadig viktigere for politiet og etterforskningsprosessen. Vi legger daglig igjen digitale fottøyavtrykk i den digitale verden. Tenker vi på hvem som kan se dette og hva det kan brukes til?

1.1 Begrunnelse for valg av tema

Med denne bacheloroppgaven ønsker vi å få en større innsikt i bevisverdien av digitale spor i en etterforskningsprosess. Under praksisåret var en av oss på lensmannskontor og den andre på politistasjon. Vi var begge innom etterforskningsavsnittet og digitale spor fanget vår interesse der. Her bemerket vi oss at digitale spor var mye mindre brukt enn hva vi hadde sett for oss før vi startet. Det var få med kompetanse på fagområdet, og ingen klare roller som kun jobbet med digitale spor på noen av praksisstedene.

Under «digitalt politiarbeid», som er et av fagene vi har første året på politihøgskolen, syntes vi begge at dette var et nyttig og spennende fag. Vår interesse for å skrive om dette temaet kom frem ved at vi både hadde bygd opp en interesse og nysgjerrighet i løpet av praksisåret, men også ble interessen fanget under «digitalt politiarbeid» som fag første året på politihøgskolen.

1.2 Valg av problemstilling

Det blir stadig viktigere at politiet har nok kunnskap om digitale spor og vi er begge interessert i å finne ut mer om dette tema. Vi valgte helseappen på bakgrunn av at det er en ny teknologi og flere saker har fått mye medieoppmerksomhet for bruk av helseappen under etterforskningen og som bevisførsel i rettssalen. Vår problemstilling er derfor: «Hvilken bevisverdi kan digitale spor generert fra helseappen på smartenheter gi i en etterforskningsprosess?»

1.3 Avgrensning

I dette prosjektet skulle vi gjerne ha sett på utallige temaer og problemstillinger, og særlig innenfor digitalt politiarbeid. Siden dette er en bacheloroppgave, ser vi oss nødt til å avgrense tema til nevnt problemstilling.

I denne oppgaven avgrenses digitale spor til å omfatte standardiserte applikasjoner på smarttelefoner og andre enheter, som genererer data til helseappen. Oppgaven vil ta for seg IOS og Android da disse utgjør 99% av de mobile operativsystemene i Norge per februar 2021 (Statcounter - GlobalStats, 2021). Siden IOS og Android har en stor markedsandel i Norge, vil det være stor sannsynlighet for at de som jobber med digitale enheter og bevissikringen fra disse, vil komme borti disse operativsystemene.

Vi vil i tillegg avgrense oppgaven til å gjelde kun for etterforskningsprosessen. Vi ser oss nødt til å gjøre dette da oppgavens begrensninger ikke gjør det mulig for oss å undersøke hele saksgangen, fra første enhet på stedet til en saksavgjørelse.

2.0 TEORI

2.1 Hva er digitale spor?

Bjerknes og Fahsing definerer digitale spor i en etterforskning-sammenheng som «data med mulig betydning for en etterforskning som er lagret digitalt og befinner seg i en elektronisk enhet» (Bjerknes & Fahsing, 2017, s. 244). Disse sporene kan fortelle oss ulike ting. Det kan si noe om den subjektive skylden, hvor noe har skjedd, hva som har skjedd, når det har skjedd og hvem som har utført handlingen (ibid).

Denne oppgaven vil omfatte digitale spor i form av metadata. Sunde presenterer metadata som "opplysninger om kommunikasjon og informasjon". Metadata er data som forteller noe om annen data (Sunde I. M., Lov og rett i cyberspace, 2006, s. 271). Smart-enhetene er programmert til å lagre data, som for eksempel skritt eller høyde forflytninger, sette dette i system og tolke dataene. Dette blir så presentert i helseappen på smarttelefonen.
Dataene i helseappen vil være permanente data, som vi vil kunne innhente fra flere år tilbake i tid, sett at brukeren har tatt i bruk enheten.

Digitale spor blir ofte lagt stor vekt på i retten, og de blir ofte sett på som nøytrale og pålitelige bevis til sammenligning med eksempelvis vitneutsagn (Bjerknes & Fahsing, 2017, s. 245).

2.2 Helsedata fra ulike smartenheter

IOS og Android genererer mye av den samme informasjonen, og vi etterlater oss digitale spor i applikasjonen og på de digitale enhetene våre. De samler blant annet inn informasjon om skritt, gå- og løpedistanse, trapper gått og søvnregistrering. Dette er noe som kan være nyttig for politiet under etterforskning av en straffesak. Vi kan ut ifra applikasjonene hente ut informasjon om brukeren og dens bevegelser. Helseappen kan også samle inn helsedata fra ulike enheter som for eksempel smartklokke og badevekt. (Samsung, 2021) (Apple, 2021).

2.3 The Digital Forensic Process

The digital forensic process er en prosess beskrevet av Flaglien. Denne prosessen består av fem faser - identifikasjon, innsamling, undersøke, analysere og presentere. Denne prosessen er

viktig for å opprettholde god notoritet, bevare bevisets integritet, prioriteringsrekkefølge og at politiets håndtering av bevis følger etablerte prinsipper og metoder. Prosessen er universell ved at den kan brukes til etterforskning av enhver straffesak eller hendelse som involverer digitale enheter (Flaglien, 2017).

2.3.1 Identifikasjon

Denne fasen handler om å identifisere potensielle beviskilder fra digitale enheter under en ransaking. Dette er en stor fase som er hypotesebasert. Her planlegger og forbereder en seg til de andre fasene.

2.3.2 Innsamling

Handler om det å få tilgang til den dataen som ønskes i aktuell sak, kopiere og klargjøre denne dataen. Her er det viktig at flyktige data, altså data som lett går tapt, sikres først. Mobiltelefoner sikres via tredjepartsprogrammer som lager en kopi av enhetens innhold.

2.3.3 Undersøke

I fase tre skal vi klargjøre dataen slik at den er leselig for oss mennesker. Her bruker vi ulike programmer som verktøy for å kunne gjøre dette. I denne fasen er det viktig å dokumentere alt man gjør, for å opprettholde notoritet i arbeidet.

2.3.4 Analyse

I denne fasen handler det om å finne og bestemme hvilke funn som styrker og svekker hypotesene og saken. Det er i denne fasen man kan si noe om hendelsen, involverte parter og vurdere hvilken bevisverdi et spor gir.

2.3.5 Presentasjon

Dette er femte og siste fase. Her utarbeider man en fullstendig rapport om utført arbeid og eventuelle funn. Det er også i denne fasen hvor man eventuelt presenterer objektive funn for retten (Flaglien, 2017, ss. 17-45).

2.4 Hvilken bevisverdi kan digitale spor gi?

I følge Fahsing og Bjerknes kan digitale spor være et selvstendig bevis i saken, eller en viktig informasjonskilde for å kunne kryss-sjekke og kontrollere en forklaring. Digitale spor som en person har lagt igjen vil som regel være mer eksakte enn en muntlig forklaring. Dette fordi digitale spor er krevende å skjule og unngå, i tillegg til at det opererer med tid. "Tidspunkt har en stor nytteverdi i digitale spor, fordi datasystemer som genererer digitale spor, ofte lagrer tidspunktet for en gitt handling" (Bjerknes & Fahsing, 2017, s. 247)

I prosessen der man samler inn datamaterialet er det viktig å isolere beviset eller datamengden og ivareta dens integritet. Bevisverdien til det digitale sporet er avhengig av politiets behandling av enhetene. For å unngå at det blir usikkerhet om eventuelle endringer bør dataene kopieres før det gjøres innsyn i dem (Sunde I. M., Databevis , 2015, s. 600).

2.5 Helseappens feilmargin

I en forskningsstudie gjort i Nederland har de studert helseapplikasjonen på tre ulike generasjoner av smartenheten iPhone. I dette studiet ble det forsket på hvor korrekt antall registrerte skritt og distanse på appen var. Forskerne varierte på hvor dem bar telefonen på kroppen, distansen og fart. Dette ble sammenlignet med antall skritt og distanse som telefonen registrerte, og hva de manuelt telte av skritt og den oppmålte virkelige distansen.

Resultatene fra studiet var at skrittene som ble registrert på iPhone sin helseapp var tilsvarende lik det som stemte med virkeligheten. Det utgjorde en feilmargin på ca. 2%. Det var flere faktorer som påvirket resultatene på en målt distanse generert fra helseappen. Dette gjorde at feilmarginen kunne bli større. Både hvordan du gikk og hvor fort du gikk hadde påvirkning på resultatet. Det viste seg at det kunne være fra 30-40% feilmargin målt på distanse som ble registrert på iPhone helseapplikasjon (Zandwijk & Boztas, 2019).

2.6 Utfordringer knyttet til digitale spor

Denne oppgaven har ikke potensiale til å gå i dybden på de mulige feilkilder som finnes knyttet til digitale spor. Vi vil i denne oppgaven presentere en oversikt over noen mulige feilkilder, herunder noen feilkilder som kan oppstå i de tre fasene innsamling, undersøke og analysere. I tillegg vil vi ta for oss mulig utfordringer knyttet til å koble enhet til person.

The digital forensics process presenterer innsamlingsfasen. I denne fasen er det flere muligheter for feilkilder. En mulig feilkilde kan være av teknisk karakter som for eksempel utfordringer med tidsstempel på enheten og tolkningsfeil i programvare når man kopierer og samler inn data fra enheten. Enhetene generer tidsstempler på de ulike dataene som lagres. Her kan det oppstå flere feilkilder ved at enheten har en feil tids-innstilling, eller at eksempelvis sikringsprogrammet overskrider tidsstemplet til enheten når det sikres og kopieres (Schatz, Mohay, & Clark, 2006).

Videre i undersøkelse- og analysefasen kan det være flere menneskelige feilkilder som oppstår. Nina Sunde og Itiel E. Dror har skrevet en forskningsartikkel som handler om at digitale bevis kan være mindre sikre enn antatt. De tar opp problematikken ved at de digitale bevisene blir preget av subjektivitet, tolkning, vurdering og valg etterforskeren på saken gjør. Dette har stor betydning for påliteligheten beviset vil ha i saken (Pileberg, 2019) (Sunde & Dror, 2019)

En siste utfordring vi har valgt å fokusere på er å knytte den digitale enheten til personen. Helseappen vil for eksempel registrere at en telefon eller smartklokke har vært i bevegelse, men ikke hvem som har hatt den med eller på seg. Derfor er det ofte at digitale bevis blir brukt for å støtte under andre bevis i saken. Fahsing og Bjerknes presenterer i boken sin at «et elektronisk spor vil sjelden kunne stå alene som bevis. Dette fordi et elektronisk spor ikke nødvendigvis knytter en enkelt person direkte til et sted eller til en handling, slik DNA eller fingeravtrykk kan gjøre» (Bjerknes & Fahsing, 2017, ss. 245-247).

3.0 METODE

3.1.0 Valg av forskningsmetode

Formålet med oppgaven var å undersøke hvilken bevisverdi data generert fra helseappen på smartenheter kan gi i en etterforskningsprosess. Dette har vi valgt å gjøre ved bruk av en kvalitativ forskningsmetode. Vi har valgt intervju som fremgangsmåte. Vi mente det ville gi oss mest utfyllende og best informasjon på forskningsfeltet, sammenlignet med kvantitativ metode som for eksempel. spørreskjema.

3.1.1 Kvalitativ metode

Det er to ulike forskningsmetoder innenfor metode, kvalitativ og kvantitative metoder. Kvalitativ metode kan for eksempel være intervju eller observasjon. «De Kvalitative metodene tar sikte på å fange opp mening og opplevelse som ikke lar seg tallfeste eller måle» (Dalland, 2017, s. 52). Kvalitative metoder kan fungere særlig godt når vi skal studere noe vi ikke vet så mye om i utgangspunktet, og som det er lite forskning på fra før av (Johannessen, Tufte, & Christoffersen, 2010, s. 32). Ved intervju vil man snakke med informantene i ettertid av en hendelse, mens ved observasjon observerer du situasjonen som en utenforstående person.

På grunn av lite forskning og artikler på tema vi valgte oss, fant vi ut at det å intervjue ulike informanter ville være en god metode for at vi skulle få mest mulig utfyllende informasjon på tema. Vi har valgt ut informanter som har jobbet ulike steder og derfor har erfaring fra flere saker. Det er viktig at man tenker over at informasjon som er hentet i etterkant ikke er rådata, slik som for eksempel. observasjon kan være (ibid). Konsekvensen ved kvalitativ metode kan blant annet være at antall informanter til prosjektet vil være lavere enn i en kvantitativ undersøkelse. I tillegg kan både intervjuet og bearbeidelsen av dataene bli i mye høyere grad påvirket av forskerens atferd, tolkning av hva som blir sagt og vurderinger forskeren gjør (Kolflaath, 2013, s. 35).

3.1.2 Utvelgelse av informanter

I prosjekter er det vanskelig å vite hvor mange personer man skal intervjue på forhånd. Mange forskere mener at du skal gjennomføre intervjuer helt til du ikke får noen ny informasjon (Johannessen, Tufte, & Christoffersen, 2010, s. 104). Siden dette er et studentprosjekt og vi

verken har tid eller kapasitet til å gjennomføre så mange intervjuer, har vi valgt å intervjue syv personer til denne oppgaven. Vi har valgt å intervjue personer med spesialkompetanse på området. Siden vi har valgt å bruke en kvalitativ tilnærming, vil utvelgelsen av informanter ikke bli tilfeldig valgt slik det ofte kan bli i kvantitative undersøkelser. I kvalitative studier er hensikten at vi skal få mest mulig informasjon og kunnskap om det vi har valgt å undersøke, og det er dette vi kaller for strategisk utvelgelse (Johannessen, Tufte, & Christoffersen, 2010, s. 106). Strategisk utvelgelse handler om at vi først må finne ut hvilken målgruppe som skal delta for at vi skal få informasjonen vi trenger, og deretter finner vi personer fra denne målgruppen som kan delta i studiet (ibid).

Informantene ble valgt ut på bakgrunn av deres kompetanse på fagfeltet. Veilederen vår på prosjektet ga oss kontaktinformasjon til flere av lederne innenfor fagfeltet, som deretter har satt oss i kontakt med informanter. I tillegg har vi selv oppsøkt ledere i andre distrikter i Norge, som videre har gitt oss kontaktinformasjon til mulige informanter. I forkant av intervjuene hadde vi kontakt med informantene på mail. Informantene fikk kun vite hvilken problemstilling vi hadde og hva vi ønsket å belyse i intervjuet. Vi valgte å ikke sende ut intervjuguiden i forkant da vi ønsket at svarene til informantene skulle være så ferske og naturlige som mulig.

3.1.3 Forberedelser og forarbeid

Det er flere forberedelser som må gjøres før et intervju. Vi laget en intervjuguide med tema og spørsmål slik at vi kunne sikre at intervjuene vi foretok oss ga svar på det vi hadde satt oss som formål med studiet. Før vi hadde intervjuene leste vi oss opp på personene, og vi hadde også fått tilsendt flere av domstols-dokumentene i sakene som informantene skulle bruke i intervjuene.

3.1.4 Semi-strukturert intervju

Vi valgte å bruke semi-strukturert intervju. Det går ut på at det benyttes en intervjuguide hvor vi hadde skrevet ned temaer og spørsmål til de ulike temaene. Et semi-strukturert intervju trenger ikke å følges til punkt og prikke. Intervjuguiden blir mer som en huskeliste der det er nedskrevet temaer og spørsmål (Johannessen, Tufte, & Christoffersen, 2010, s. 139). Et semi-strukturert intervju ga oss mye fleksibilitet og vi kunne bevege oss frem og tilbake i intervjuguiden. Dette gjorde at intervjuet ble mer levende og vi kunne få mer informasjon på spørsmålene, enn hva et strukturert intervju kunne gitt oss.

3.1.5 Utvikling av intervjuguide

Vi valgte å ha en åpen struktur, men med en intervjuguide som en slags huskeliste. Det gjorde at vi kunne ha en god struktur og holde en rød tråd gjennom intervjuene, og få svar på temaene vi hadde satt oss. Vi utarbeidet intervjuguiden ved å hente ut inspirasjon fra både tidligere leverte bacheloroppgaver og masteroppgaver. Vi hadde hele tiden i bakhodet at vi måtte ha med spørsmål som kunne svare på problemstillingen vår. Intervjuguiden besto hovedsakelig av åpne spørsmål slik at vi fikk mest mulig informasjon fra informantene.

3.1.6 Pilottest av intervjuguide

Pilottest av intervjuguiden handler om å holde et test-intervju. Vi valgte å teste dette på en ansatt i politiet, som har kunnskap innenfor tema. Dette for at vi kunne få et tilnærmet likt intervju som vi skulle gjennomføre senere i prosjektet vårt. Ved å ta en test kunne vi finne ut av hvor lang tid vi brukte, om noen av spørsmålene var overflødig, om vi trengte å legge til noen spørsmål og om vi trengte å endre på rekkefølge på spørsmål og/eller temaene vi hadde satt oss. Etter pilotintervjuet så vi oss nødt til å legge til et spørsmål hvor vi spurte om hvilke typer saker informantene har brukt helseappen i en etterforskningsprosess.

3.1.7 Gjennomføring av intervju

Intervjuene til dette prosjektet ble gjennomført i en tidsperiode på to uker. Det ble gjort lydopptak av alle intervjuene. Vi tok alle intervjuene sammen, hvor vi byttet på å skrive og stille spørsmål. Vi mener denne måten ga oss en bredere forståelse, det var lettere å følge med og det ga oss et godt utgangspunkt for oppfølgingsspørsmål. Informantene ble intervjuet en og en over en videotjeneste. Intervjuene tok alt i fra 45 minutter til 2 timer.

Informantene var engasjert og interessert i å dele informasjon og sin kunnskap med oss. Vi valgte å intervjue kun spesialister innenfor fagområdet, og ser i etterkant at dette var nødvendig for å belyse problemstillingen vår på en god måte. Flere av svarene vi fikk fra informantene var relativt like, noe som vil være med på å underbygge vår problemstilling.

Dersom vi hadde hatt mer tid på dette prosjektet ville vi intervjuet flere informanter for å få mer empiri, og gå dypere inn i materien som problemstillingen omfavner. Dette er et tema som er dagsaktuelt og som stadig er under utvikling. Det vil derfor være nødvendig med mer forskning på fagområdet.

3.1.8 Metodologiske refleksjoner

Med en kvalitativ tilnærming ønsker man å oppnå høy grad av validitet og pålitelighet, og man prøver å få det fenomenet man skal undersøke så virkelighetsnært som mulig. Forskningsmetoden vi valgte for dette prosjektet var intervju. Når man har en empirisk tilnærming, herunder intervju, kan det oppstå noen utfordringer.

En faktor vi i ettertid har reflektert over, som kan ha vært utfordrende, er å ha intervju over videotjenester. Dette ga oss både tekniske utfordringer, og det ga oss en utfordring ved at vi ikke fikk den naturlige kontaktetableringen med intervjuobjektene. Vi startet hvert intervju med å stille noen innledende spørsmål for å bli litt kjent med informantene, og for å bygge en slags relasjon oss imellom. Vi fikk en god forståelse av hverandre og kommuniserte bra, sett bort ifra at det var over videotjeneste. Likevel kan det ha vært med på å påvirke intervjuene våre.

Relasjonen mellom intervjuobjektet og vi som intervjuer kan også være en annen faktor som vil kunne påvirke våre resultater. Informantene skal tolke spørsmålene vi stiller, og vi skal tolke den informasjonen informantene kommer med. Et intervju handler om å kommunisere med hverandre. I kommunikasjon er det rom for at det skapes misforståelser og feiltolkninger på hva som blir sagt. Dette kan føre til at påliteligheten til den informasjonen som kommer frem under intervjuet blir svekket (Johannessen, Tufte, & Christoffersen, 2010, s. 147). For å forebygge dette valgte vi å ta alle intervjuene sammen. Vi opplevde at vi måtte utdype og forklare spørsmålene om igjen, da vi ikke alltid følte at informantene tolket spørsmålene vi stilte på rett måte.

3.1.9 Etiske hensyn

«Etikk handler først og fremst om forholdet mellom mennesker, det vil si spørsmål om hva vi kan og ikke kan gjøre mot hverandre» (Johannessen, Tufte, & Christoffersen, 2010, s. 89). Når vi skal utføre et prosjekt som for eksempel foregår med intervju, vil dette direkte berøre mennesker. Vi må derfor være bevisst at etiske problemstillinger kan oppstå. For at menneskene skal bli ivaretatt på best mulig måte må vi følge noen etiske standarder og retningslinjer. Noen av retningslinjene er utarbeidet av den nasjonale forskningsetiske komite for samfunnsvitenskap og humaniora (NESH). En av retningslinjene omhandler at deltakerne i prosjektet har rett til å bestemme selv over egen deltakelse, og har rett på å trekke seg uten å

nevne noen grunn (De nasjonale forskningsetiske komiteene, 2016).

I forkant av intervjuene fikk informantene utdelt et samtykkeskjema som forklarer hvordan informasjonen ville bli brukt og lagret. De fikk også informasjon om at de uten begrunnelse kan trekke samtykket sitt. Informantene fikk informasjon om hva prosjektet skulle handle om og anonymisering. Skjemaene ble signert og sendt til oss.

Vi har valgt å ikke ha med personsensitive opplysninger, slik at informantene ikke kan bli gjenkjent og identifisert gjennom prosjektet vårt. For å unngå etiske problemer har vi heller ikke stilt personsensitive spørsmål, og vi har meldt prosjektet vårt til Norsk senter for forskningsdata (NSD).

3.2 Analyse av funn

Braun og Clarke (2013) har utviklet en analysemetode for å strukturere informasjonen fra blant annet intervjuer på en hensiktsmessig og ryddig måte. Vi valgte å benytte oss av denne metoden, da vi vurderte den som oversiktlig og enkel. Dette for å kunne analysere dataene vi har hentet inn slik at vi på en systematisk og hensiktsmessig måte lettere kunne finne ut hvilke funn som var viktig å vektlegge og hvilke som var mindre viktige.

Braun og Clark presenterer i sin metode seks steg for å enklere kunne analysere dataen man innhenter i prosjektet. Disse seks stegene omhandler å finne likhetstrekk ved dataene man har funnet, før man koder dataene om til ulike temaer. Etter at temaene er delt inn, vil det være enklere å se ulike utsagn og temaer som skiller seg ut. På denne måten vil man raskt kunne finne fellesnevnere fra informantene, noe som vil bli viktig for prosjektet videre. Etter man har kommet frem til de ulike temaene som man anser som de mest sentrale, er det viktig å gå over og se at utsagnene informantene har kommet med er satt til riktig tema. Til slutt kan man begynne å definere punktene under temaene mer. Her skal det under hvert tema skrives en detaljert analyse og forklare hvilken informasjon som fremkommer fra hvert tema (Clarke & Braun, 2013).

4.0 RESULTATER

4.1 Presentasjon av data

Vi valgte å intervjue syv informanter, hvor alle jobbet i politiet. Alle informantene hadde spesialiststillinger innenfor digitalt politiarbeid i ulike distrikter. Dette ga oss et bredt spekter og et representativt utvalg i form av spesialister. Noen av informantene hadde mer erfaring med data fra helseappen enn andre, og dette kan ha påvirket resultatene i denne oppgaven.

Vi vil i dette kapittelet presentere erfaringen og kompetansen til de ulike informantene, hvordan de ser på bevisverdien av helsedata, og hvilke utfordringer de har erfart. Vi vil benytte oss av direkte sitater fra informantene, for å understreke våre funn. Av hensyn til informantene og deres jobb, vil de i denne oppgave bli anonymisert og vi vil bruke navn som informant 1, informant 2 osv. Vi har delt opp intervjuet i ulike temaer etter analysemetoden til Braun og Clarke. Etter vi transkriberte intervjuene visualiserte vi klare fellesnevnere på flere av temaene, og dette skal vi presentere i dette kapittelet.

4.2 Erfaring og kompetanse

Det første tema vi har delt intervjuet opp i handlet om informantenes erfaring med bruk av helsedata og hvilken kompetanse de hadde på fagområdet. Våre informanter fortalte at de hadde erfaring med bruk av helsedata i straffesaker. Samtlige informanter fortalte at de hadde brukt helsedata i saker med høy alvorlighetsgrad, og at det sjeldent eller aldri hadde blitt brukt i saker med lav alvorlighetsgrad. Informant 7 forteller:

> "Jeg har opplevd å bruke helsedata i noen trafikkulykker, men utover dette har jeg kun brukt det i alvorlige trafikkulykker og andre mer komplekse saker. Jeg jobber på et spesialavsnitt så sakene er filtrert når vi får anmodning om bistand for å gå gjennom digitale beslag i saken. Hvis jeg hadde jobbet et annet sted ville det mest sannsynlig være mye mer variert".

Videre forteller informant 2: "Vi har brukt helseappen i flere ulike type saker. Vi på dette avsnittet har ikke kapasitet til å ta oss av de små sakene, så det blir i utgangspunktet kun de mer komplekse sakene, altså de sakene som er prioritert fra Riksadvokaten. Vårt avsnitt involveres aldri i eksempelvis vinningssaker". Vi opplevde på bakgrunn av disse funnene at

samtlige av informantene vi intervjuet svarte at de kun hadde jobbet med mer komplekse saker.

Informantene hadde alle spesialisert kompetanse og vi forsto det slik at de hadde mye erfaring og kunnskap på fagområdet. Det var varierende hvor lenge de hadde jobbet med digitalt politiarbeid, men samtlige ga uttrykk for at de hadde en forståelse for helsedata og funksjonen av dette.

4.3 Bevisverdien av bruk av data fra helseappen i en etterforskningsprosess

Videre i intervjurundene snakket vi med informantene om bevisverdien de mente helsedata hadde i etterforskningsprosessen. Det var flere av informantene som fortalte at man måtte se helsedata i sammenheng med andre bevis. Informant 7 eksemplifiserer dette på følgende måte:

> "Jeg ser på verdien av helsedata som høy. Det har ikke nødvendigvis en høy egenverdi, men det vil være indisier man knytter opp mot øvrige bevis i saken. Ofte er det så mye data, og generell enhetsbruk i tillegg, at du kan knytte sammen data og se en hel historie. Du ser for eksempel at brukeren har løftet opp telefonen, skjermen går på og brukeren låser opp telefonen ved bruk av ansiktsgjenkjenning. Vedkommende skriver så en melding med innholdet "jeg kommer om 10 minutter". Deretter ser du at personen har gått 15 skritt bort i gangen, stått stille i et gitt tidsrom, og gått opp en trapp. Det er mye som skal til for at den informasjonen ikke stemmer, dersom man gjør det på en ordentlig måte"

Samtlige av informantene fortalte at helsedata isolert sett har liten bevisverdi i etterforskningsprosessen og saksgangen ellers, men sett i sammenheng med andre opplysninger i en straffesak vil det kunne ha høy bevisverdi. Informant 2 fortalte: "Jeg vil si at i det store og det hele er det et godt supplement i mange saker. Det er sjeldent helsedata står alene. Alene er det vanskelig å si at det har høy bevisverdi".

Vi fikk oppfatning av at noen av informantene var svært opptatt av å bruke helsedata med forsiktighet og i tillegg bruke helsedata både for å svekke en hypotese så vel som å styrke en hypotese. Informant 5 forteller dette:

> "Det er viktig å bruke helsedata i begge retninger. Det er nøytral og steril informasjon som kan være med på å styrke eller svekke en mistanke. Viktig å være oppmerksom på hva man kan få ut av helseappen, og bruke det med forsiktighet".

Under intervjuene ble informantene spurt om hvilke spor fra helseappen som ga størst bevisverdi og som ble mest brukt i straffesaker. Det var noe forskjell i svarene informantene ga oss. Flere av informantene anså skritt som mest nøyaktig og mente at dette ble mest brukt i straffesakene. Informant 4 forteller: "Antall steg er noe av de dataene man kan stole mest på, mens etasjer gått er noe usikkert. Vi har testet dette selv med Iphone og så at det må være en høy nok etasje for at appen skal registrere den. Jeg tror det var rundt 10-12 steg som måtte til for at en etasje skulle bli registrert".

Andre informanter var mer skeptisk til å peke ut enkelte data fra helseappen. De fortalte at det var viktig å avdekke om det var skritt eller andre bevegelser som hadde gjort at det ble registrert skritt i helseappen. Informant 6 illustrerer dette ved:

> "Forskningen sier at skritt er veldig nøyaktig og at det er en feilmargin på ca.2%. Det er en viktig presisering at dette er hvis det faktisk er gått skritt. Man må da positivt vite at enheten har vært et sted på kroppen som gjør det nøyaktig og at det er gått skritt. Hvis du da finner 100 skritt på en telefon og du sier at det er 2% nøyaktighet, men så viser det seg at det er sykling så kan det ende opp med å være 3 km i stedet for".

4.4.0 Utfordringer med bruk av data fra helseappen i en etterforskningsprosess

Det siste tema vi valgte å ta for oss i intervjurundene var hvilke utfordringer som kan oppstå ved bruk av data fra helseappen i etterforskningsprosessen. Utfordringer henger tett sammen med hvilken bevisverdi helsedata utgjør i etterforskningsprosessen. For å få en bedre innsikt i hvilken bevisverdi helsedata kan ha, og hvilke utfordringer det fører med seg, valgte vi å stille spørsmål om informantene så noen utfordringer knyttet til bruken av helseappen.

4.4.1 Utfordring rundt registrering av helsedata

Informant 2 fortalte at en utfordring som kunne oppstå ved bruk av helsedata var at det er mye usikkerhet rundt registreringen av eksempelvis antall skritt og distanse som er gått. Informant 2 eksemplifiserer det slik:

> "Man må være bevisst på tolkningen av helsedata. Ta eksempelvis distanse. Står det at vedkommende har gått en kilometer, så trenger det ikke være at det er en kilometer. Det kan variere veldig i forhold til hvordan enheten er plassert på kroppen, om vedkommende har gått i ring og på skrittlengde. Det er mange faktorer som påvirker registreringen i helseappen".

4.4.2 Utfordring med tidsstempling

Videre fortalte flere av informantene at en annen utfordring med bruk av helsedata kan være at verktøyene som brukes for å kopiere dataene på enheten kan ha tolket tidsstemplet feil. I tillegg kan klokken på enheten være stilt inn feil. Informant 4 forklarer dette på følgende måte:

> "Helsedataene lagres i databasefiler på telefonen, og det er ulike databaser tilknyttet direkte til operativsystemet. Eksempelvis er IOS veldig flinke til å være nøyaktige på tiden. I dag er det en standardisert innstilling på telefonen som gjør at enheten stiller seg etter den tidssonen enheten er i. Det vi pleier å sjekke når vi sikrer en telefon er å skru på skjermen og sjekke tid/dato på enheten. Deretter sammenlignes dette med en nettside som viser atomtiden, nøyaktig tid. Da ser man om det er noe forskjeller. Er det ingen forskjell har eksempelvis IOS innstilt at det er riktig tid på klokken. Jeg har ikke opplevd til nå at det er store avvik i tidsstempel på IOS-enheter. Dersom det har vært avvik har det i så tilfelle vært snakk om 1 eller 2 sekunder".

Vi oppfattet fra flere av informantene at tid på enheten ikke var et stort problem og at telefonene som regel var riktig innstilt i forhold til tiden. Informant 1 forklarer det på denne måten:

> "Fordelen med mobiltelefoner nå i dag er at de synkroniseres med nettverket sitt, og vil da ofte være rett. Men vi ser fortsatt at det kan være feil på tidsinnstillinger. Når vi får inn telefoner kontrollerer vi tidsinnstillingene som er på enheten, men vi kan ikke med 100% sikkerhet si at det er sånn tidsinnstillingene var når det straffbare forholdet skjedde. Det er sjeldent nå at folk bruker noe annet enn automatisk tidsinnstilling på telefonen".

4.4.3 Utfordring med manglende kompetanse og lagring av helsedata

En annen utfordring vi har sett er at data lett kan bli overskrevet av annen data, dersom man ikke får sikret telefonen raskt nok eller at telefonen ikke blir tatt i beslag på riktig måte. Vi oppfattet at informantene mente dette da handlet om manglende kompetanse fra de som ikke jobber med digitale bevis til daglig. Informant 1 hadde et eksempel på dette fra en sak hen hadde jobbet med, informant 1 forklarer:

> "I en sak jeg var borte i hadde vedkommende blitt pågrepet av politiet ikke lenge etter hendelsen. Politiet hadde da tatt med seg personen, med telefonen i lomma, på en liten rundtur. De skulle innom bopel for å hente noen ting, og var også innom flere plasser med pågrepne i bilen. På bakgrunn av dette kunne man se bevegelser fra hvor de hadde vært. Dette kunne ført til at enheten overskrev data som allerede var lagret på telefonen, og kunne resultert i tap av viktig data".

Under intervjurundene ble vi oppmerksom på at det ikke fantes noe system eller oversikt over hvor lenge de forskjellige dataene lagres på en enhet. Vi forsto det slik at helsedata ble lagret lenger enn for eksempel annen enhetsbruk. Informant 4 forklarer:

> "Helsedata lagres lenger og man kan se 1-2 måneder tilbake i tid. Men ved etterforskning på seksjonsnivå blir sakene liggende lenge, og kan vare i for eksempel 1 år. Dersom telefonen ikke blir sikret tidlig nok, kan det være at informasjon har blitt overskrevet eller slått sammen. Du vil da i stedet for å få informasjon om at mellom klokken 10-11 gikk du x-antall skritt, vil dataene slås sammen og gi en total på antall skritt gått den dagen".

4.4.4 Menneskelige feilkilder

Informantene tok i tillegg til tekniske feilkilder opp menneskelige feilkilder. Vi satt igjen med en oppfatning om at det er mye avhengig av etterforsker, og hvordan etterforskere tolker de digitale bevisene. Informant 6 forteller: "Det er lett å falle i fella for å lese mye mer ut av det enn hva det egentlig er. Man må ikke bruke det mer enn hva det faktisk sier".

4.4.5 Å knytte enhet til person

Under intervjurundene var vi interessert i å finne ut hvordan informantene har jobbet i sine saker, med å knytte enhet til person. Flere av informantene syntes ikke at dette var et problem

i sine saker, men at det er et viktig punkt i etterforskningsprosessen. Dette for at man skal vite at man har riktig gjerningsperson, og at ingen andre har brukt telefonen til vedkommende under gjerningstidspunktet. Informant 3 forteller:

> "For oss var det veldig enkelt, da vi i forkant av pågripelse hadde navn på enhetene, og kontroll på hvem som eide enhetene. Det var også e-poster knyttet til vedkommende og masse brukernavn. Her var det lett å knytte enhet til riktig person. Dersom man ikke har informasjon om dette i forkant må man gå inn og se på andre ting på enheten i samme tidsrom, som kan knytte person til enheten.. Dette vil da være å se på flere spor som meldinger, anrop og innlogging på tjenester"

Vi oppfattet det slik at flere av informantene mente at man måtte være forsiktig med å kun bruke helsedata for å knytte enhet til person. Informant 6 forteller:

> "Det er viktig å ha i bakhodet at man ikke trenger å låse opp telefonen for å generere skritt. Noen kan ha tatt telefonen og løpt 100 meter for så å legge telefonen tilbake. Dette kan skje i veldig mange tilfeller. Noen kan også ha tatt et kredittkort, brukt det, og lagt det tilbake igjen".

5.0 EMPIRISK ANALYSE

I denne delen av oppgaven vil vi koble våre funn opp mot teorien vi tidligere har nevnt som vil styrke/svekke våre funn og resultater.

I teorikapittelet ble the digital forensic process presentert. Dette er som nevnt en prosess som omhandler håndtering og sikring av digitale bevis (Flaglien, 2017). Det er viktig å følge denne prosessen for å ivareta bevisets integritet og verdi. Vi kan se at det er flere utfordringer med helsedata som kan forekomme i de ulike fasene. Vi vil i dette kapittelet tolke våre funn og se hvilken data fra helseappen som kan gi størst bevisverdi. I tillegg vil vi se på bevisverdien til helsedata isolert sett og sett i sammenheng med andre opplysninger i en straffesak.

Videre i dette kapittelet vil vi bruke den overnevnte prosessen sammen med teori for å analysere våre funn.

5.1 Identifikasjonsfasen

Politidirektoratet (2012) presenterer i sin rapport at datatekniske undersøkelser på åstedet kan være helt avgjørende for å kunne oppklare ulike saker og benyttes av og til i alvorlige saker og drapssaker. Videre i rapporten trekkes det frem at elektroniske spor står sentralt i flere større saker de siste årene. I en rapport fra Politidirektoratet (2017) fremgår det at datamengden i verden øker stadig mer og mer. Når datamengden øker, så vil utbredelsen av elektroniske spor også øke (Politidirektoratet, 2012) (Politiet, 2017).

I identifikasjonsfasen handler det om å identifisere potensielle beviskilder under blant annet ransaking (Flaglien, 2017, s. 16). Dette kan være for eksempel digitale spor på en mobiltelefon. Denne oppgaven omhandler helsedata, og det vil dermed være det vi bruker som eksempel. I denne fasen er det viktig at politibetjentene som er på stedet gjør en grundig jobb og innehar digital forståelse. Det vil være en fordel for saksløsning å vite om at mobiltelefoner genererer helsedata ut ifra bevegelsene personen foretar seg. Informant 1 sier: «Det handler om å være litt kreativ. Man må kunne tenke på hva som kan motbevise eller støtte under det vedkommende sier. Kanskje man må tenke litt utenfor boksen?».

Når en politibetjent tar beslag i en enhet er det viktig at man følger metoder for å best ivareta eventuelle spor og bevis på enheten. Dette gjøres ved at enheten blir satt i flymodus (Bergum,

2017) eller lagt i en faraday bag (Faraday AS, 2019). Informant 4 fortalte at det er viktig å vite at selv om mobilen blir satt i flymodus, så kan enheten fortsatt generere bevegelse og dermed helsedata. Dette kan gjøre bruken av helsedata sårbart. I tillegg til dette vil en mobil som blir lagt i en faraday bag hele tiden søke etter signaler, noe som gjør at den fortere går tom for strøm, og kan miste data dersom den slår seg av.

Som nevnt tidligere under resultater hadde informant 1 et eksempel der hen belyser problemstillingen som omhandler mangelen på digital kompetanse hos politibetjenter. Ut fra teorien vi har sett på tidligere og rapportene som POD presenterer ser vi at det ikke er noen tvil om at digitale spor er viktig å ha kompetanse om og behandle med forsiktighet.

5.2 Innsamlingsfasen

Videre i prosessen fra Flaglien presenterte vi innsamlingsprosessen. Dette er den fasen det blir viktig å få tilgang til, kopiere og klargjøre den dataen som ønskes i aktuell sak. Våre informanter ble spurt om hvordan de fikk tilgang på denne dataen, og hva som eventuelt trengs. I korrespondanse mellom PHS og riksadvokaten presiserte riksadvokaten at innholdet på mobilen sikres ved å ta en speilkopi av beslaget, som vil si at gjennomgang av speilkopien er å anse som ransaking av beslaget (Brev fra Riksadvokaten til Jon Aga (PHS), 21.04.2020, Ransaking av databærere). Informantene våre anså det ikke som noen utfordring å få denne tilgangen, og siden alle informantene fikk anmodninger fra politidistriktene var grunnlaget om rettslig tilgang allerede vurdert.

I innsamlingsprosessen kan det oppstå utfordringer med tekniske feilkilder. I teorikapittelet presenterte vi en utfordring ved at enheten har en feil tidsinnstilling, eller at sikringsprogrammet overskrider tidsstemplet til enheten. I en forskningsartikkel skrevet av Bradley Schatz og Andrew Clark forklares det at det kan være utfordrende med tidsstempling på enheter som ikke er synkronisert med internett og at tidssoner også er en utfordring (Schatz, Mohay, & Clark, 2006).

Flere av informantene våre på den andre siden mente at tidsstempler i dag er ganske nøyaktige. Vi tolket det til at så lenge den som sikrer mobiltelefonen først, er flink til å kontrollere tid og dato på enheten når enheten blir tatt i beslag, er det ikke et stort problem.

Informantene mente at tidsstempling kunne være en utfordring, men at de ikke hadde opplevd det selv og det heller ikke har blitt et spørsmål i rettssalen.

Ut ifra teorien har vi forstått det slik at tidsstempling er en stor utfordring, men det er ikke slik vi tolker våre funn. Vi tolker det slik at det kan være en utfordring, men at informantene ikke har opplevd det selv. Vi har forstått det slik at det er viktig å ha i bakhodet, og vite om viktigheten av å sjekke dato og tid. Dette for å bevare bevisets integritet, riktighet og verdi.

5.3 Undersøkelsesfasen

I undersøkelsesfasen presenterer Flaglien viktigheten av notoritet i arbeidet man gjør for å klargjøre datamengden fra de elektroniske sporene. I denne fasen kan det oppstå flere utfordringer.

Nina Sunde og Itiel E. Dror presenterer i sin artikkel en utfordring som omhandler menneskelige feilkilder. I artikkelen vektlegger Sunde og Dror at de elektroniske sporene kan bli preget av subjektivitet, tolkning, vurdering og valg etterforskeren på saken gjør (Sunde & Dror, 2019). Inntrykket vi fikk fra informantene var at det ikke var et gjennomgående problem hos spesialistene, men at det kunne være utfordrende når andre skulle tolke deres funn. Informant 7 eksemplifiserte dette ved:

> "Først og fremst er en utfordring hvilken kompetanse etterforskeren på saken sitter med. Det er veldig fort gjort å mistolke data og en annen utfordring kan være kompetansen til de som sitter i retten. Det kan være en etterforsker som har feiltolket dataene og aktor, forsvarer og dommer som ikke har kompetanse til å forstå hva vi snakker om. Det blir ofte banale spørsmål fra disse. "Er det han som gjorde dette her eller ikke". De har ikke kompetanse til å utfordre de tekniske bevisene og det er veldig skummelt. Jeg har selv opplevd å være vitne i en sak hvor dommer, forsvarer eller aktor ikke hadde noe som helst grunnlag for å stille kritiske spørsmål. Da ble jeg egentlig veldig overrasket. Det som er skummelt i de tilfellene er at jeg kunne sagt hva som helst og blitt trodd. Hadde ikke jeg hatt kompetanse til det og feiltolket dataene kunne det gått utover rettssikkerheten".

Videre i denne fasen blir viktigheten av å undersøke hvem som tilhører enheten. Fahsing og Bjerknes forklarer i boken sin at det kan være mer utfordrende å knytte elektroniske spor til

en persons handling og plassering, enn DNA og fingeravtrykk (Bjerknes & Fahsing, 2017, ss. 245-247).

Biometri er et viktig hjelpemiddel, og da også særlig for politiet. Dette brukes til å fastslå identitet og knytte personer til et åsted. Biometri er beskrevet som kjennetegn som utgår fra kroppen. Kjennetegnene er unike for oss som enkeltindivider og samtidig permanente og stabile over tid. De mest kjente er blant annet fingeravtrykk og ansiktsform (Datatilsynet, 2019). Smarttelefoner i dag bruker ofte biometri som autentisering. Dette kan for eksempel være bruk av fingeravtrykk eller ansiktsgjenkjenning. For at man skal kunne knytte en person til enheten kan det være aktuelt å undersøke om hvordan enheten har blitt låst opp på det aktuelle tidspunktet. Er telefonen blitt låst opp med biometri eller kode? Eller er mobilen ikke blitt låst opp i det hele tatt? Om det sistnevnte er tilfelle kan dette være en indikasjon i seg selv på at man må belyse hvem telefonen tilhører og om gjerningsperson har brukt telefonen i det aktuelle tidsrommet. Informant 3 eksemplifiserte dette på følgende måte:

> "Vi hadde en sak hvor gjerningspersonen hadde latt mobilen ligge igjen i leiligheten sin, med et spill gående. Dette gjorde han for å kunne bruke det som alibi i ettertid at han spilte spill hjemme. Det vi så var at mobilen ikke hadde registrert noen bevegelser i helseappen, og ei heller blitt låst opp. Dette gjorde at mangel på registrering ble et bevis i seg selv. Vi testet det i etterkant og helseappen registrerer bevegelse tross av at en sitter i senga og spiller spill på mobilen".

Ut fra det Sunde og Dror presenterer ser vi tydelig at det er nødvendig for mer kompetanse og forståelse på fagområdet. Vi ser at det er tydelig utfordrende dersom etterforskere, dommere, forsvarere og aktor ikke innehar kompetanse til å stille kritiske spørsmål. Dette blir enda mer utfordrende for politiet fordi kravene til kompetanse når det gjelder personvern og teknisk sikkerhet er omfattende. Vi er av den oppfatning at blant annet jurister mangler forståelse for de tekniske spissfindigheter og gråsoner som teknologien enten ivaretar eller ikke ivaretar.

Vi satt igjen med et inntrykk av at man må være en IKT sikkerhetsspesialist og at økt kompetanse på området er nødvendig. I tillegg kan det gå utover bevisets verdi da det ikke blir brukt og belyst slik andre bevis i straffesaker blir.

Videre ser vi at biometri kan være et viktig bevismiddel og henger tett sammen med andre bevis som eksempelvis helsedata. Vi forstår det slik at verdien på helsedata kan øke dersom smarttelefonen har blitt låst opp med biometri underveis på gjerningstidspunktet, og det gjør det i tillegg lettere å knytte enheten til person på det aktuelle tidspunktet.

5.4 Analysefasen

I analysefasen blir det beskrevet av Flaglien at det handler om å finne og bestemme hvilke funn som styrker og svekker hypotesene som er opprettet i straffesaken (Flaglien, 2017). Det er i denne fasen man vurderer hvilken bevisverdi helsedata kan gi.

Som nevnt i teorikapittelet skriver Fahsing og Bjerknes at digitale spor sjeldent kan stå alene som bevis. Våre funn viser at samtlige av våre informanter nevner at helsedata sjeldent eller aldri har eller kan stå alene som bevis i en straffesak. Informant 6 fortalte at "det er mye som må kunne kryss-sjekkes for at helsedata skal kunne bli brukt i en straffesak. Helsedata er objektiv og steril informasjon, men det må bli satt i sammenheng med for eksempel avhør eller andre opplysninger i straffesaken".

I en forskningsstudie gjort i Nederland ble det forsket på hvor korrekt antall registrerte skritt og distanse på appen var (Zandwijk & Boztas, 2019). Resultatet fra studien viste at skritt var den mest nøyaktige dataen, og at det var større unøyaktighet rundt distanse. Våre funn støtter opp under denne studien og flere av informantene hadde gjort egne undersøkelser som ga samme resultat som studien. Informantene fortalte oss at de aldri hadde brukt distanse da det var for stor unøyaktighet rundt dataen, og at det ville gitt lav bevisverdi. Registrerte skritt ble derimot brukt hyppigere og samtlige av informantene fortalte oss at skritt-registrering ga god bevisverdi.

En utfordring som ble nevnt var at selv om skritt-registrering hadde god bevisverdi, var det utrolig lett å manipulere mobilen til å registrere skritt. Det ble nevnt at mobilen kunne ligge i bilen på en humpete vei eller at man kunne riste på mobilen og likevel generere skritt. Uavhengig av dette sa samtlige informanter at det hadde god bevisverdi sammen med andre opplysninger i saken.

Våre funn satt opp mot forskningsstudiet fra Nederland viser at deler av helse-dataene gir god bevisverdi sett i sammenheng med andre opplysninger i saken, men vil være vanskelig å bruke og gir lavere bevisverdi alene.

5.5 Presentasjonsfasen

Dette er den siste fasen i Flagliens prosess. Her utarbeider man en rapport om utført arbeid og eventuelle funn.

Som nevnt kan det i denne fasen oppstå en utfordring med presentasjon av data i retten. Ved at dommer, aktor eller forsvarer ikke har kunnskap nok til å kunne stille kritiske spørsmål, kan det gjøre at rettssikkerheten blir satt på prøve. Flere av informantene våre nevnte også at en utfordring her kunne være etterforskers forståelse av rapporten. Etterforsker på saken får tilsendt rapport fra spesialistene og tolker informasjonen feil. Dette gjør at bevis kan bli brukt feil i saken. Videre nevner informantene at dette handler om etterforskerens forståelse for digitale spor, og at det ikke alltid er like lett å holde følge med utviklingen av digitale spor.

5.6 Styrker og svakheter ved studien vår

I dette prosjektet har vi hatt både tids-, og ordbegrensning som kan ha vært med på å svekke studiet vårt. Dette er et forskningsfelt som er i stadig utvikling, vi har analysert menneskers oppfatninger av bevisverdien til helsedata og vi mener det vil være behov for videre forskning på dette feltet. Vi har valgt å forske på noe som er relativt nytt, og som det fortsatt er lite kunnskap om. Vi vurderer det slik at det å ha valgt ut folk som besitter høy kompetanse på fagområdet, og har gitt oss god informasjon.

Det hadde vært spennende å kunne intervjue flere personer, og i tillegg kunne intervjue de samme personene om noen måneder igjen, da de vil kunne ha enda mer erfaring på fagområdet.

I tillegg er det viktig å være kritiske til den metoden man har valgt å bruke. Dersom vi hadde valgt å bruke en kvantitativ tilnærming til prosjektet ville dette kunne medført til andre resultater. Vi kunne ha fått et bredere spekter i svarene våre og flere svar, men vi kunne ikke stilt like utdypende spørsmål slik vi har kunnet gjøre med intervju. Vi vurderte det slik at det var viktigere for oss å få dypere informasjon, enn omfanget av data man får fra kvantitative

undersøkelser som for eksempel et spørreskjema. Vi valgte å intervjue syv informanter til vårt prosjekt, og vi syntes det ga oss et godt datagrunnlag. Dersom vi hadde intervjuet enda flere, hadde vi fått sett enda flere perspektiver og fått enda mer empiri som kunne styrket studien vår.

Vi har kun intervjuet personer med spesialkompetanse på fagfeltet, og som jobber med større saker. Dette har kunne gjort at vi har gått glipp av informasjon om bruken av helsedata i saker med lavere alvorlighetsgrad og kompleksitet. Dette er en svakhet ved studiet vårt, og noe som vi anbefales at det forskes mer på.

6.0 KONKLUSJON

I dette kapittelet i oppgaven vil vi svare på problemstillingen vår. Målet med studiet har vært å se på hvilken bevisverdi digitale spor fra helseappen som genereres fra smartenheter, kan gi i en etterforskningsprosess. Vi har lagt informantenes opplevelser og oppfatninger til grunn i konklusjonen, og viser ovenfor til at videre studie rundt dette fagområdet vil være nødvendig.

Når samfunnet er i stadig endring og digitale spor blir stadig viktigere i straffesaker er det viktig med økt fagekspertise. Vi har i dette studiet forsøkt å gi en overordnet beskrivelse av noen av feilkildene. Det er viktig å vite at ulike IKT løsninger har ulike feilkilder, noe som kan gi ulike fagekspertiseutfordringer.

Våre funn indikerer at det er viktig med kompetanse og forståelse for digitalt politiarbeid hos flere aktører i politiet, og at viktigheten av dette øker og øker. Ut ifra studiet vårt ser vi at det blir viktig for politiet å ha tilgang til tverrfaglig kompetanse for å kunne bygge korrekt bevisførsel i straffesaker. Behandlingen av digitale spor fra helseappen blir viktig for hvilken bevisverdi helseappen vil ha i etterforskningsprosessen.

For at man skal bruke helsedata som bevis i en straffesak vil det være flere faktorer som spiller inn og som må belyses i etterforskningsprosessen for at politiet skal kunne føre korrekt bevisførsel. Vi har sett på flere feilkilder, utfordringer, oppfatninger og forskning på fagfeltet.

Kildene vi har brukt i utredningen indikerer at politiet må utvikle omfanget av kompetansen og kapasitet for å møte fremtidens behov. Våre funn har tydeliggjort at indikert utvikling bør være basert på videre forskning knyttet til hvordan tverrfaglige team kan etableres for å støtte the digital forensic process. Det bør forskes på organiseringen av politiet for en fremtid der digitale spor vil kunne utgjøre en større andel av etterforskningsgrunnlaget. Det forutsetter at denne tematikken ikke er utredet tidligere.

Basert på vår studie og våre funn vil vi per dags dato anta at helseappen gir høy bevisverdi sammen med andre opplysninger i straffesaken, og lavere bevisverdi alene.

7.0 LITTERATURLISTE

Apple. (2021). *Bruk Helse-appen på iPhone eller iPod touch*. Hentet fra Support Apple - lest: 17.01.2021: https://support.apple.com/no-no/HT203037

Bergum, U. (2017). Kriminalteknikk - Første enhet på åstedet. I E. H. (red.), *Kriminalteknikk - Første enhet på åstedet* (ss. 209-233). Oslo: Gyldendal Norsk Forlag AS.

Bjerknes, O. T., & Fahsing, I. A. (2017). I *Etterforskning - prinsipper, metoder og praksis* (ss. 242-278). Fagbokforlaget.

Clarke, V., & Braun, V. (2013, Februar). *Teaching thematic analysis: Overcoming challenges and developing strategies for effective learning.* Hentet fra ResearchGate - lest: 28.01.2021: https://www.researchgate.net/publication/269928387_Teaching_thematic_analysis_Overcoming_challenges_and_developing_strategies_for_effective_learning/link/549962170cf22a831396056c/download

Dalland, O. (2017). I *Metode og oppgaveskriving* (ss. 51-60). Gyldendal akademisk.

Datatilsynet. (2019, 07 17). *Biometri*. Hentet fra Hva er en personopplysning? - lest: 06.03.2021: (https://www.datatilsynet.no/rettigheter-og-plikter/personopplysninger/biometri/

De nasjonale forskningsetiske komiteene. (2016, April, 4.utgave). *Forskningsetiske retningslinjer for samfunnsvitenskap, humaniora, juss og teologi.* Hentet fra Forskninsetikk - lest: 28.01.2021: https://www.forskningsetikk.no/globalassets/dokumenter/4-publikasjoner-som-pdf/forskningsetiske-retningslinjer-for-samfunnsvitenskap-humaniora-juss-og-teologi.pdf

Faraday AS. (2019). *Faraday shielding*. Hentet fra Faraday shielding - lest:14.03.2021: https://www.faraday.no/faraday-shielding

Flaglien, A. O. (2017). The Digital Forensics Process. I A. Årnes, *The Digital Forensics Process* (ss. 13-49). John Wiley & Sons, Incorporated.

Johannessen, A., Tufte, P. A., & Christoffersen, L. (2010). I *Introduksjon til samfunnsvitenskapelig metode* (ss. 27-34, 35-51, 89-98, 103-116, 135-162, 163-172). Polen: Abstrakt forlag AS.

Kolflaath, E. (2013). I *Bevisbedømmelse i praksis* (ss. 25-39). Bergen: Fagbokforlaget.

NSD. (Lest 2020). *Samtykke og andre behandlingsgrunnlag*. Hentet fra Personverntjenester - lest: 18.12.2020: https://www.nsd.no/personverntjenester/oppslagsverk-for-personvern-i-forskning/samtykke-og-andre-behandlingsgrunnlag/ (

Pileberg, S. (2019, Juni 23). *Digitale bevis kan være mindre sikre enn antatt*. Hentet fra Forskning - lest: 21.01.2021: https://forskning.no/partner-politi-politihogskolen/digitale-bevis-kan-vaere-mindre-sikre-enn-antatt/1349209

Politidirektoratet. (2012, Juli 10). *Elektroniske spor, IKT-kriminalitet og politiarbeid på internett.* Hentet fra Politiet i det digitale samfunnet - lest: 18.02.2021: https://medlem.ntl.no/Content/103500/cache=20122109105334/Politiet%20i%20det%20digitale%20samfunn%20juli%2012.pdf

Politiet. (2017, 12 15). *Politi- og lensmannsetatens kapasitets- og kompetansebehov de kommende ti-årene.* Hentet fra Politiet - lest: 18.02.2021: https://www.politiet.no/globalassets/04-aktuelt-tall-og-fakta/bemanning-ressurser-og-dekningsgrad/bemanning-og-dekningsgrad/politi--og-lensmannsetatens-kapasitets--og-kompetansebehov-de-kommende-ti-arene.pdf

Samsung. (2021). *Samsung Health*. Hentet fra Samsung - lest: 17.01.2021: https://www.samsung.com/no/apps/samsung-health/

Schatz, B., Mohay, G., & Clark, A. (2006). *A correlation method for establishing provenance of timestamps in digital evidence*. Hentet fra Digital Investigation - lest: 14.02.2021: https://www.sciencedirect.com/science/article/pii/S1742287606000715

Statcounter - GlobalStats. (2021, Februar). Hentet fra Mobile Operating System Market Share in Norway - lest: 11.02.2021: https://gs.statcounter.com/os-market-share/mobile/norway

Sunde, I. M. (2006). I *Lov og rett i cyberspace* (s. 271). Bergen: Fagbokforlaget.

Sunde, I. M. (2015). Databevis . I R. Aarli, M.-A. Hedlund, & S. E. (Red.), *Bevis i straffesaker - utvalgte emner* (ss. 599-633). Oslo : Gyldendal Norsk Forlag AS.

Sunde, N., & Dror, I. E. (2019, Juni). *Cognitive and human factors in digital forensics: Problems, challenges, and the way forward*. Hentet fra Digital Investigation - lest: 18.02.2021: https://www.sciencedirect.com/science/article/pii/S1742287619300441?via%3Dihub

Zandwijk, J. P., & Boztas, A. (2019, April). *The iPhone Health App from a forensics perspective: can steps and distances registered during walking and running be used as digital evidence?* Hentet fra Digital Investigation - lest: 11.01.2021: https://www.sciencedirect.com/science/article/pii/S1742287619300313

7.1 Selvvalgt pensum

Apple. (2021). *Bruk Helse-appen på iPhone eller iPod touch*. Hentet fra Support Apple - lest: 17.01.2021: https://support.apple.com/no-no/HT203037 **(2s.)**

Clarke, V., & Braun, V. (2013, Februar). *Teaching thematic analysis: Overcoming challenges and developing strategies for effective learning.* Hentet fra ResearchGate - lest: 28.01.2021: https://www.researchgate.net/publication/269928387_Teaching_thematic_analysis_Overcoming_challenges_and_developing_strategies_for_effective_learning/link/549962170cf22a831396056c/download **(13s.)**

Datatilsynet. (2019, 07 17). *Biometri*. Hentet fra Hva er en personopplysning? - lest: 06.03.2021: (https://www.datatilsynet.no/rettigheter-og-plikter/personopplysninger/biometri/ **(3s.)**

De nasjonale forskningsetiske komiteene. (2016, April, 4.utgave). *Forskningsetiske retningslinjer for samfunnsvitenskap, humaniora, juss og teologi.* Hentet fra Forskninsetikk - lest: 28.01.2021: https://www.forskningsetikk.no/globalassets/dokumenter/4-publikasjoner-som-pdf/forskningsetiske-retningslinjer-for-samfunnsvitenskap-humaniora-juss-og-teologi.pdf **(44s.)**

Faraday AS. (2019). *Faraday shielding*. Hentet fra Faraday shielding - lest:14.03.2021: https://www.faraday.no/faraday-shielding **(3s.)**

Johannessen, A., Tufte, P. A., & Christoffersen, L. (2010). I *Introduksjon til samfunnsvitenskapelig metode* (ss. 27-34, 35-51, 89-98, 103-116, 135-162, 163-172). Polen: Abstrakt forlag AS. **(58s.)**

Kolflaath, E. (2013). I *Bevisbedømmelse i praksis* (ss. 25-39). Bergen: Fagbokforlaget. **(14s.)**

NSD. (Lest 2020). *Samtykke og andre behandlingsgrunnlag*. Hentet fra Personverntjenester - lest: 18.12.2020: https://www.nsd.no/personverntjenester/oppslagsverk-for-personvern-i-forskning/samtykke-og-andre-behandlingsgrunnlag/ **(4s.)**

Pileberg, S. (2019, Juni 23). *Digitale bevis kan være mindre sikre enn antatt*. Hentet fra Forskning - lest: 21.01.2021: https://forskning.no/partner-politi-politihogskolen/digitale-bevis-kan-vaere-mindre-sikre-enn-antatt/1349209 **(5s.)**

Politidirektoratet. (2012, Juli 10). *Elektroniske spor, IKT-kriminalitet og politiarbeid på internett.* Hentet fra Politiet i det digitale samfunnet - lest: 18.02.2021:

https://medlem.ntl.no/Content/103500/cache=20122109105334/Politiet%20i%20det%20digitale%20samfunn%20juli%2012.pdf **(33s.)**

Politiet. (2017, 12 15). *Politi- og lensmannsetatens kapasitets- og kompetansebehov de kommende ti-årene.* Hentet fra Politiet - lest: 18.02.2021: https://www.politiet.no/globalassets/04-aktuelt-tall-og-fakta/bemanning-ressurser-og-dekningsgrad/bemanning-og-dekningsgrad/politi--og-lensmannsetatens-kapasitets--og-kompetansebehov-de-kommende-ti-arene.pdf **(50s.)**

Samsung. (2021). *Samsung Health*. Hentet fra Samsung - lest: 17.01.2021: https://www.samsung.com/no/apps/samsung-health/ **(4s.)**

Schatz, B., Mohay, G., & Clark, A. (2006). *A correlation method for establishing provenance of timestamps in digital evidence*. Hentet fra Digital Investigation - lest: 14.02.2021: https://www.sciencedirect.com/science/article/pii/S1742287606000715 **(10s.)**

Statcounter - GlobalStats. (2021, Februar). Hentet fra Mobile Operating System Market Share in Norway - lest: 11.02.2021: https://gs.statcounter.com/os-market-share/mobile/norway **(1s.)**

Sunde, I. M. (2006). I *Lov og rett i cyberspace* (s. 271). Bergen: Fagbokforlaget. **(26s.)**

Sunde, I. M. (2015). Databevis . I R. Aarli, M.-A. Hedlund, & S. E. (Red.), *Bevis i straffesaker - utvalgte emner* (ss. 599-633). Oslo : Gyldendal Norsk Forlag AS. **(34s.)**

Sunde, N., & Dror, I. E. (2019, Juni). *Cognitive and human factors in digital forensics: Problems, challenges, and the way forward*. Hentet fra Digital Investigation - lest: 18.02.2021: https://www.sciencedirect.com/science/article/pii/S1742287619300441?via%3Dihub **(8s.)**

Zandwijk, J. P., & Boztas, A. (2019, April). *The iPhone Health App from a forensics perspective: can steps and distances registered during walking and running be used as digital evidence?* Hentet fra Digital Investigation - lest: 11.01.2021: https://www.sciencedirect.com/science/article/pii/S1742287619300313 **(8s.)**

- **320 sider - refererer til kunngjøring Canvas 11.02.21**

8.0 VEDLEGG

Vedlegg 1: Godkjennelse fra NSD

NSD NORSK SENTER FOR FORSKNINGSDATA

NSD sin vurdering

Prosjekttittel

Bacheloroppgave

Referansenummer

121963

Registrert

19.12.2020 av [redacted]

Behandlingsansvarlig institusjon

Politihøgskolen

Prosjektansvarlig (vitenskapelig ansatt/veileder eller stipendiat)

Robert Andre Furuhaug, robert.furuhaug@phs.no, tlf: 92411103

Type prosjekt

Studentprosjekt, bachelorstudium

Kontaktinformasjon, student

[redacted]

Prosjektperiode

01.09.2020 - 30.06.2021

Status

22.01.2021 - Vurdert

Vurdering (1)

22.01.2021 - Vurdert

Det er vår vurdering at behandlingen av personopplysninger i prosjektet vil være i samsvar med personvernlovgivningen, så fremt den gjennomføres i tråd med det som er dokumentert i meldeskjema med vedlegg 22.1.2021, samt i meldingsdialogen mellom innmelder og NSD. Behandlingen kan starte.

FORUTSETNINGER FOR VURDERINGEN
Setningen «Prosjektet er meldt til Personvernombudet ved NSD.» må fjernes fra informasjonsskrivet,

ettersom NSD ikke er personvernombud for Politihøgskolen. Det er ikke nødvendig å laste opp revidert informasjonsskriv i meldeskjemaet.

MELD VESENTLIGE ENDRINGER
Dersom det skjer vesentlige endringer i behandlingen av personopplysninger, kan det være nødvendig å melde dette til NSD ved å oppdatere meldeskjemaet. Før du melder inn en endring, oppfordrer vi deg til å lese om hvilke type endringer det er nødvendig å melde:
https://nsd.no/personvernombud/meld_prosjekt/meld_endringer.html

Du må vente på svar fra NSD før endringen gjennomføres.

TYPE OPPLYSNINGER OG VARIGHET
Prosjektet vil behandle alminnelige kategorier av personopplysninger frem til 30.6.2021.

LOVLIG GRUNNLAG
Prosjektet vil innhente samtykke fra de registrerte til behandlingen av personopplysninger. Vår vurdering er at prosjektet legger opp til et samtykke i samsvar med kravene i art. 4 og 7, ved at det er en frivillig, spesifikk, informert og utvetydig bekreftelse som kan dokumenteres, og som den registrerte kan trekke tilbake.

Lovlig grunnlag for behandlingen vil dermed være den registrertes samtykke, jf. personvernforordningen art. 6 nr. 1 bokstav a.

PERSONVERNPRINSIPPER
NSD vurderer at den planlagte behandlingen av personopplysninger vil følge prinsippene i personvernforordningen om
- lovlighet, rettferdighet og åpenhet (art. 5.1 a), ved at de registrerte får tilfredsstillende informasjon om og samtykker til behandlingen
- formålsbegrensning (art. 5.1 b), ved at personopplysninger samles inn for spesifikke, uttrykkelig angitte og berettigede formål, og ikke viderebehandles til nye uforenlige formål
- dataminimering (art. 5.1 c), ved at det kun behandles opplysninger som er adekvate, relevante og nødvendige for formålet med prosjektet
- lagringsbegrensning (art. 5.1 e), ved at personopplysningene ikke lagres lengre enn nødvendig for å oppfylle formålet

DE REGISTRERTES RETTIGHETER
NSD vurderer at informasjonen om behandlingen som de registrerte vil motta oppfyller lovens krav til form og innhold, jf. art. 12.1 og art. 13.

Så lenge de registrerte kan identifiseres i datamaterialet vil de ha følgende rettigheter: innsyn (art. 15), retting (art. 16), sletting (art. 17), begrensning (art. 18) og dataportabilitet (art. 20).

Vi minner om at hvis en registrert tar kontakt om sine rettigheter, har behandlingsansvarlig institusjon plikt til å svare innen en måned.

FØLG DIN INSTITUSJONS RETNINGSLINJER
NSD legger til grunn at behandlingen oppfyller kravene i personvernforordningen om riktighet (art. 5.1 d), integritet og konfidensialitet (art. 5.1. f) og sikkerhet (art. 32).

For å forsikre dere om at kravene oppfylles, må dere følge interne retningslinjer og eventuelt rådføre dere med behandlingsansvarlig institusjon.

OPPFØLGING AV PROSJEKTET
NSD vil følge opp ved planlagt avslutning for å avklare om behandlingen av personopplysningene er

avsluttet.

Lykke til med prosjektet!

Kontaktperson hos NSD: Lasse Raa
Tlf. personverntjenester: 55 58 21 17 (tast 1)

Vedlegg 2: Intervjuguide

INTERVJUGUIDE

«Hvilken bevisverdi kan digitale spor generert fra helseappen på smartenheter gi i en etterforskningsprosess?».

MÅL: Finne ut hvilken bevisverdi helse-appen har for etterforskere, i en etterforskningsprosess.

Innledende spørsmål: (Skal ikke brukes til noe i oppgaven - kun kontaktetablering!)

1. Alder
2. Hvilken erfaring har du i politiet og fra tidligere?
3. Hvilken utdanning og evt. ekstra kurs har du?
    a) hvilken utdanning har du fått forut stillingen som etterforsker/spesialist?
4. Fortell litt om din stilling og dine arbeidsoppgaver.
5. Hvor mange år har du jobbet i etaten?
6. Hvor lang tid som etterforsker/spesialist?

Hovedspørsmål

1. Fortell litt om dine erfaringer om bruk av data fra helseappen på smartenheter i en etterforskningsprosess.

2. Hvilken type informasjon/datamateriale kan du få ut av helseappen?
    a) Har du sett noe forskjell på informasjon/datamateriale på forskjellige enheter? Samsung, Apple osv. IOS -ANDROID
    b) Kan du forklare litt om de forskjellige type dataene du kan hente ut fra helse-appen?
    c) Er det noen type data som blir mer brukt, og som har høyere bevisverdi enn andre?

3. Hvilke data fra helse-appen har du kompetanse til å analysere?
    a) hvordan utfører du denne prosessen?
    b) Er noe data fra helseappen du tenker kan gå tapt på grunn av manglende kompetanse?

4. Hva kreves for at man skal få tilgang til data fra helseappen?
    a) Utstyr?
    b) Lovhjemler det er tuftet på

5. Hvilke typer saker har du brukt helseappen i en etterforskningsprosess? (INN I INTERVJUGUIDE ETTER PILOTTEST)
    a) Har du kun brukt data fra helseappen i store etterforskningssaker?
    b) Kan du komme med noen eksempler?
    c) Uforholdsmessig

6. Hvordan ser du på verdien av bruk av data fra helseappen i en etterforskningsprosess?
    a) «Hvilken bevisverdi ser du ved bruk av data fra helseappen i etterforskningen og kan du komme med noen eksempler?».

7. Ser du noen utfordringer med bruk av helseappen i en etterforskningsprosess?
    a) Har du erfart at det er noen feilkilder i forbindelse med denne bruken? Tekniske og menneskelige.
    b) Hvordan har du fått knyttet enheten til person?
        1. Hvilke utfordringer er det med dette?
    c) Ser du noen utfordringer med tanke på tid, på enheten?
    d) Ressurser og prioritering, små VS store saker?

Vedlegg 3: Informert samtykke skjema

SAMTYKKESKJEMA

til intervjudeltakere

Samtykke til å delta i bachelorprosjekt *«Hvilken bevisverdi kan digitale spor fra helse-appen, som genereres fra smartenheter, gi i en etterforskningsprosess?»*

Som bachelorstudenter ved Politihøgskolen [redacted] skal vi gjennomføre et prosjekt med mål om å beskrive bevisverdien som digitale spor generert fra smartenheter kan ha i en etterforskningsprosess. Prosjektet blir veiledet av Robert André Furuhaug (Robert.furuhaug@phs.no), ved Politihøgskolen [redacted]

Deltakelsen i bachelorprosjektet *«Hvilken bevisverdi kan digitale spor fra helse-appen, som genereres fra smartenheter, gi i en etterforskningsprosess?»* innebærer at du vil bli intervjuet i om lag en times tid. Intervjuene foretas av bachelorstudenter [redacted] og [redacted] og vil være en åpen dialog med særlig fokus på hvilke faktorer som er og har vært av betydning for deg når det gjelder «elektroniske spor i forbindelse med etterforskningsprosessen». Det vil bli benyttet båndopptaker/PC for opptak av intervjuene, som kun undertegnede har tilgang til. Lydfiler fra båndopptaker vil overføres til en sikkerhetsbeskyttet PC og slettes ved prosjektets slutt, senest juni 2021. Bachelorprosjektet er underlagt taushetsplikt og alle opplysninger blir behandlet konfidensielt. Resultatet av intervjuene vil presenteres anonymisert, og det vil ikke bli gitt spesifikk informasjon som kan spores tilbake til den enkelte informant eller tjenestested.

Utvalget er valgt ut ifra kunnskap og kompetanse om temaet i prosjektet. Vi har fått kontaktopplysninger fra både veileder på prosjektet og kontakter vi har privat i etaten.

Så lenge du kan identifiseres i datamaterialet, har du rett til:

- innsyn i hvilke opplysninger som er registrert om deg, og å få utlevert en kopi av opplysningene,
- å få rettet personopplysninger om deg,
- å få slettet personopplysninger om deg, og
- å sende klage til personvernombudet om behandlingen av dine personopplysninger.

Kontaktopplysning personvernombudet politihøgskolen: personvernombud@phs.no

Det er helt frivillig å delta i prosjektet. Du kan på hvilket som helst tidspunkt trekke deg uten å måtte begrunne beslutningen nærmere.

På oppdrag fra Politihøgskolen [redacted] har NSD – Norsk senter for forskningsdata AS vurdert at behandlingen av personopplysninger i dette prosjektet er i samsvar med personvernregelverket.

Er det spørsmål i forbindelse med denne henvendelsen, eller ønskes det informasjon om resultatene når de foreligger, kan undertegnede kontaktes.

Med vennlig hilsen

[redacted]
Bachelorstudenter Politihøgskolen [redacted]
Tlf: [redacted]
Epost: [redacted]

Samtykkeerklæring

Jeg har mottatt informasjon om bachelorprosjektet ««*Hvilken bevisverdi har digitale spor som genereres fra helseappen på smarttelefoner i etterforskningsprosessen?*»?» og er villig til å delta i prosjektet.

Dato: .....

Signatur:..... Telefonnummer:.....