UiO : Det juridiske fakultet

Politiets tilgang til elektroniske spor

Utlevering av elektronisk lagrede data til politiet etter personvernreglene og de straffeprosessuelle regler

Kandidatnummer: 585

Leveringsfrist: 25. April 2017

Antall ord: 15361

Innholdsfortegnelse

1 Innledning

Vi legger igjen stadig flere elektroniske spor med vår bruk av alt fra mobiltelefoner og datamaskiner til bruk av bilen og betalinger. Stadig flere tjenester blir digitaliserte og automatiserte og mange tilbydere av ulike tjenester registrerer mye data om oss. Big Data-analyser kan i stadig større grad brukes for å identifisere hvem vi er og hvilke preferanser vi har[1]. Dette setter personvernet på prøve og gir samtidig økte muligheter for bruk av elektroniske spor i etterforskningen av straffbare forhold. Denne oppgaven vil belyse politiets tilgang til enkelte elektroniske spor under personvernlovgivningen og straffeprosessen.

1.1 Oppgavens tema

Opptak fra kameraovervåkning, bompasseringsdata, trafikkdata, og data om betalingstransaksjoner er verdifulle spor i etterforskingen av straffesaker. Der slike bevis kan knyttes til en konkret person, kan de si mye om en persons bevegelser og kommunikasjon knyttet til relativt presise tidsangivelser. Oppgaven tar sikte på å belyse rettsreglene som gjelder for politiets tilgang til disse opplysningene under etterforskningen. Det disse ulike typene elektroniske spor har felles er at dataene lagres hos den som leverer tjenesten der opplysningene registreres. Dette er opplysninger som genereres når vi beveger oss i et område med kameraovervåkning, passerer en bomstasjon, bruker mobiltelefon eller internett eller foretar betalinger og kontantuttak. Det er opplysninger om våre bevegelser og vår bruk av ulike tjenester som registreres, men vi har ikke kontroll på dataene selv. De ligger lagret hos den som foretar registreringen av bruken vår. Det vil være den som har eier mobiltelefonnettet, bompengeselskapet, den som har satt opp overvåkningskamera og banken vi bruker. Det at opplysningene registreres om noen, men lagres hos andre, gjør at det er to parter som kommer i betraktning når politiet har behov for opplysningene, den personen opplysningene er registrert om og det selskapet som har registrert opplysningene.

Som et utgangspunkt kunne man tenke seg å anvende beslag eller utleveringspålegg, jf. bestemmelsene i straffeprosessloven kapittel 16. Det forutsetter at opplysningene er å anse som «ting», jf. strpl. § 203 og § 210, noe som behandles senere i oppgaven. Det følger av strpl. § 205 første ledd at beslag besluttes av påtalemyndigheten for ting som besitteren «ikke vil utlevere frivillig». For de nevnte data vil besitteren typisk være samarbeidsvillig overfor politiet. Opplysningene som er lagret er imidlertid generert som følge av en annen persons aktivitet, og spørsmålet er da hvorvidt besitteren har kompetanse til å samtykke til utlevering når politiet ber om det.

[1] NRK (2017)

Opplysningene må som utgangspunkt antas å være personopplysninger jf. personopplysningsloven § 2 nr. 1. Det er dermed nærliggende å først kartlegge hvilken frihet besitteren har til å utlevere opplysningene etter personopplysningslovens regler. I den utstrekning man ikke når frem etter dette regelverket, er det behov for å beskrive den straffeprosessuelle fremgangsmåten. Etter min mening er temaet velegnet for å bli belyst for bedre å se sammenhengen mellom regelverkene.

1.2 Metode

I denne oppgaven har jeg anvendt den alminnelige rettskildelære for å fastlegge gjeldende rett innenfor de tema oppgaven belyser. Det er tre proposisjoner jeg har brukt en god del. Det er forarbeidene til personopplysningsloven i Ot.prp. nr. 92 (1998-1999), forarbeidene til ekomloven i Ot.prp. nr. 58 (2002-2003) og forarbeidene til gjennomføring av Datalagringskonvensjonen i norsk rett i Prop. 49L (2010-2011). Endringene ved gjennomføring av Datalagringskonvensjonen har ikke trådt i kraft, men proposisjonen behandler dagens praksis angående sikring av elektroniske spor ved beslag og utleveringspålegg samt en del statistiske data om bruken av reglene til innsamling av elektroniske spor og er således relevant.

Ved tolkning av personvernreglene må Den Europeiske Menneskerettighetskonvensjonen (EMK) artikkel 8 tas i betraktning. EMK er integrert i norsk lovgivning og fungerer som selvstendige regler og som tolkningsfaktor ved andre rettsregler, herunder også reglene i personopplysningsloven og straffeprosessloven. En hver inngripen i personvernet kreves særskilt hjemmel og personopplysningslovens formål er å beskytte disse interessene.

Politiet har ingen generell fullmakt til å gripe inn i den personlige sfære og reglene om politiets inngripen må ikke tolkes for utvidende eller brukes analogisk. Dette setter sitt preg på metoden innenfor straffeprosessen. I straffeprosessen gjelder det materielle sannhetsprinsipp og rettssikkerhetsprinsippene som overordnede retningsgivende hensyn ved fortolkningen av de enkelte bestemmelsene. Ved anvendelsen av tvangsmidler står hensynet til etterforskningen mot personvernhensyn. Vurderingen om betingelsene for inngrep er tilstede innebærer en avveining av disse hensynene gjennom forholdsmessighetsprinsippet, som er inkorporert i strpl. § 170a.

Oppgavens problemstillinger er knyttet til personopplysningslovens regler for behandling av personopplysninger sett i sammenheng med de straffeprosessuelle regler for beslag og utlevering. Personopplysningsloven kom i år 2000 og erstattet den tidligere personregisterloven. Loven kom til etter et grundig arbeid av personregisterutvalget[2] som ble behandlet av depar-

[2] NOU 1997:19 (1997).

tementet i Ot.prp. nr. 92 (1998-1999). Bestemmelsene om behandling av personopplysninger har i liten grad vært behandlet av domstolene. Det er to saker som har vært behandlet i høyesterett, hvorav den ene blir behandlet under kapittel 3.3.3, ni saker har vært behandlet i lagmannsretten og syv i tingretten.[3]

Personopplysninger behandles ikke bare etter reglene i personopplysningsloven. Det er mange personopplysninger som også er underlagt lovbestemt taushetsplikt. Taushetsplikten må ses i sammenheng med reglene i personopplysningsloven. Oppgaven vil ta for seg hvordan reglene for taushetsplikt etter ekomloven og finansforetaksloven påvirker politiets tilgang til å få ellers taushetsbelagte opplysninger utlevert. Da kommer blant annet reglene om vitneplikt etter straffeprosessloven. § 108 og reglene om vitne- og beslagsforbud etter straffeprosessloven §§ 117 flg og § 204 i betrakting. Ekomloven regulerer virksomheten til alle leverandører av elektroniske kommunikasjonstjenester og elektroniske kommunikasjonsnettverk. Finansforetaksloven regulerer virksomheten i finansforetak. Finansforetakene forestår betalingstjenester og betalingstransaksjoner etter finansavtaleloven.

Politiets etterforskning av straffesaker, herunder innhenting av bevis, er regulert i straffeprosessloven. Reglene i straffeprosessloven om beslag (§ 203) og utleveringspålegg (§ 210) kom med straffeprosessloven av 1981 og er i hovedsak en videreføring av tidligere § 212 og § 216 i straffeprosessloven av 1887. Reglene omtales i liten grad i forarbeidene. § 210 ble supplert med et nytt andre ledd ved lov av 3. Desember 1999 nr 82, som gir påtalemyndigheten hastekompetanse til å kreve bevis utlevert dersom det er fare ved opphold. Beslutningen skal i slike tilfelle snarest mulig forelegges retten for godkjennelse. Det er gjennom årene etablert en betydelig rettspraksis til bestemmelsene om beslag og utleveringspålegg. Det er registrert 65 publiserte dommer fra høyesterett knyttet til strpl. § 203 i lovdata og 32 tilvarende dommer knyttet til § 210.[4]

1.3 Oppbygning av oppgaven

Oppgaven tar for seg reglene for politiets tilgang til opptak fra kameraovervåkning, data fra bompasseringer, data om betalingstransaksjoner og trafikkdata. En viktig side ved politiets tilgang til elektroniske spor som er registrert hos en annen en den opplysningene gjelder er om den registrerte samtykker til at politiet skal få tilgang til opplysningene. Samtykkeproblematikken blir drøftet gjennomgående gjennom oppgaven.

[3] tall fra søk i Lovdata 2. mars 2017

[4] tall fra søk i Lovdata 2. mars 2017

Den første problemstillingen oppgaven reiser er om reglene for behandling av personopplysninger åpner for at besitteren frivillig kan gi politiet tilgang til opplysningene under personvernreglene. Der disse reglene ikke gir hjemmel for utlevering vil oppgaven videre ta for seg reglene for utlevering av personopplysninger under straffeprosessloven bestemmelser og hvordan situasjonen arter seg der de aktuelle opplysningene er underlagt lovbestemt taushetsplikt.

De forskjellige kategoriene elektroniske spor oppgaven omhandler vil falle inn under ulike deler av regelverket. Oppgaven vil belyse hvordan disse forskjellene bringer spørsmålet om utlevering av opplysningene inn under ulike bestemmelser.

1.4 Avgrensninger

Der oppgaven omhandler behandling av personopplysninger etter reglene i personopplysningsloven vil behandling av sensitive opplysninger etter personopplysningsloven § 9 faller utenfor oppgavens tema. Selv om det antas at kameraopptak, bompasseringsdata, trafikkdata, og data om betalingstransaksjoner er personopplysninger jf. personopplysningsloven § 2 nr 1 så vil de ikke bli klassifisert for sensitive. Sensitive opplysninger er definert i personopplysningsloven § 2 nr 8 og er typisk mer skjermingsverdig informasjon som etnisk bakgrunn, politisk ståsted, helseforhold mv.

Under de straffeprosessuelle regler vil oppgaven i hovedsak omhandle politiets tilgang til elektroniske spor ved beslag og utleveringspålegg og bare overfladisk behandle andre regler der de er relevante for sammenstillingen. Oppgaven vil ikke omhandle regler for sikring og utlevering av data under kommunikasjon eller fremtidig lagrede data som beskrevet i straffeprosesslovens kapitler 16a, 16b og 16d. Der oppgaven avgrenses mot andre regler vil disse bli behandlet i det enkelte kapittel.

Det er flere typer elektroniske spor som ikke behandles i oppgaven, slik som data fra kommunikasjonskontroll, innholdsdata fra lagringsmedier mv. og en fullstendig oppstilling i en oppgave av dette omfang ville medført en ganske overfladisk presentasjon av de enkelte typer. En oppgave som omhandler elektroniske spor som er lagret hos en tjenestetilbyder kunne typisk tatt med de data som lagres hos tjenestetilbydere på internett som Google, Facebook mv. Den problemstillingen ville imidlertid være av et slikt omfang at den er mer egnet for en egen oppgave enn å sammenstilles med trafikkdata mv. Derfor vil ikke spor vi legger igjen hos tilbydere på internett omfattes av oppgaven selv om de definitivt vil falle inn under den definisjonen av elektroniske spor som brukes i oppgaven.

2 Elektroniske spor

Elektroniske spor er ikke et rettslig begrep og brukes ikke som betegnelse i straffelovgivningen. Begrepet "elektroniske spor" i denne oppgaven vil i stor grad være synonymt med begrepet "elektronisk lagrede data" slik det fremkommer i straffeprosessloven § 215a. Regelen i § 215a kom inn i straffeprosessloven ved en lovendring i 2005 som gjennomfører Datakrimkonvensjonen[5] i norsk rett. Straffeprosessloven § 215a implementer konvensjonens artikkel 16 og 17 i norsk rett. Slik begrepet "elektronisk lagrede data" er brukt i § 215a kan et sikringspålegg bare omfatte data som allerede er lagret hos besitteren. Det kan tenkes at andre vil ta med data under kommunikasjon i begrepet "elektroniske spor", slik som data fra kommunikasjonsovervåkning, men det faller utenfor den betydningen begrepet er ment å ha i denne oppgaven, jf. avgrensingen i kapittel 1.4.

Begrepet "data" kan defineres som "digital informasjon i form av elektronisk maskinlesbare signaler ment for automatisk behandling i et datasystem". Data i denne form kan overføres mellom datamaskiner i et nettverk eller lagres på fysiske lagringsmedier. Elektronisk lagrede data, slik det beskrives over, vil omfatte data som er lagret på et lagringsmedium og som inneholder informasjon som kan leses og gi en betydning som kan tolkes av mennesker ved hjelp av dataprogrammer.

I rettspraksis[6] har betegnelsen "databærer" blitt brukt i flere saker som henvisning til et lagringsmedium som inneholder lagrede data. Det har sin analogi til de elektroniske spor som omhandles i denne oppgaven, ved at de elektroniske sporene er lagret på databærere i en dataserver. Der politiet tar beslag i databærere er det for å sikre det lesbare innholdet som bevis.
Opplysninger fra kameraopptak, bompengeanlegg, elektronisk kommunikasjon og betalingstransaksjoner vil i utgangspunktet være elektronisk lagrede data og hver enkelt av dem beskrives under.

2.1 Kameraovervåkning

Kameraovervåking er bruk av videokamera til å overvåke det som skjer innenfor videokameraets rekkevidde. Dette kan gjøres med eller uten bruk av opptak, men opptak av overvåkningen vil nok være mest vanlig. I motsatt tilfelle vil man være avhengig av å ha noen til å se på bildene fra overvåkningskameraene mer eller mindre hele tiden samt at man da ikke kan ha

[5] Europarådets konvensjon om bekjempelse av kriminalitet som knytter seg til informasjons- og kommunikasjonsteknologi

[6] Se blant annet Rt 2011 s. 1188 og Rt 2012 s. 1645

behov for bildene i etterkant. For at kameraovervåking skal ha en nytte som bevis i straffesaker vil det nødvendigvis betinge at det er tatt opptak.

Opptak fra kameraovervåking trenger ikke være lagret digitalt som data. Med dagens teknologiske løsninger med digitale kameraer og lagringsenheter vil nok likevel digital lagring være mest vanlig. Det skal ikke utelukkes at det fremdeles finnes analoge løsninger for kameraovervåking som sikrer opptak på videokassetter, men det vil nok medføre sjeldenhetene. Også analoge opptak er lagret med en elektronisk løsning selv om den ikke er databasert. Personopplysningslovens regler skiller ikke mellom kameraovervåkning som er lagret digitalt eller analogt og oppgaven vil heller ikke gjøre et slikt skille.

2.2 Bompasseringsdata

Bompasseringsdata er digitalt lagret informasjon om kjøretøy som passerer en bomstasjon som har automatisk registrering av passeringer. I dag er det stadig mer vanlig at bompengeanlegg har helautomatisk registrering av at alle passerende kjøretøy slik at det ikke er mulig med manuell betaling for passering. De helautomatiske bomstasjonene registrer informasjon fra en abonnementsenhet i kjøretøyet, en såkalt Autopass-brikke. Når det passerer kjøretøy som ikke har en slik Autopass-brikke blir det tatt et bilde av fronten av kjøretøyet som viser registreringsnummeret slik at bompengeselskapet kan fakturere etterskuddsvis. Bomstasjonene registrer bare opplysninger om kjøretøy som har kjennetegn både foran og bak. Motorsykler registreres ikke.

Bompasseringsdata inneholder en kode for bompengeanlegget som passeres, dato og tidspunkt for passeringen og hvilket kjøretøy som passerer basert på identiteten til Autopassbrikken som er montert i kjøretøyet eller foto av registreringsnummer.[7] I bompengeanlegg som registrerer betaling for passering i begge retninger, vil hver retning registreres som en egen bomstasjon.[8]

Data om bompasseringene lagres i bompengeanlegget normalt i opptil et døgn, men vil lagres opp til 72 timer ved behov. Etter dette overføres dataene til Statens Vegvesens sentrale register. Dataene lagres i utgangspunktet i fem år i henhold til dagens bokføringsregelverk, men det tilbys også såkalt sporfri avtale der opplysningene blir fortløpende slettet.[9]

Der det er registrert bompasseringsdata vil de gi konkrete opplysninger om hvor et kjøretøy har befunnet seg på et bestemt tidspunkt og hvilken retning kjøretøyet har beveget seg. Bevis-

[7] Autopass (2016)

[8] Statens Vegvesen (2017)

[9] Statens Vegvesen (2017)

verdien i slike data er knyttet til selve kjøretøyets bevegelser. Dataene gir ingen informasjon om hvem som fører kjøretøyet, om det er passasjerer i kjøretøyet eller hvem passasjerene er. Politiet må kunne dokumentere eller sannsynliggjøre på annet vis hvem kjøretøyet kan knyttes til på det konkrete tidspunkt.

2.3 Trafikkdata

Straffeprosessloven bruker både begrepet kommunikasjonsdata i strpl. § 210b tredje ledd og trafikkdata i strpl. § 215a femte ledd for å beskrive data om elektronisk kommunikasjon. Det er mange måter å kategorisere data på og Sunde[10] skiller blant annet mellom data som er lagret (informasjon) og data som er under overføring (kommunikasjon). Begrepet "trafikkdata" vil i denne oppgaven omhandle de data en leverandør av elektroniske kommunikasjonsnett lagrer om trafikken som går i kommunikasjonsnettverket. Begrepet er bevisst valgt for å avgrense mot kommunikasjonsavlytting, som i tillegg til trafikkdata vil omfatte innholdet i kommunikasjonen.

Begrepet "trafikkdata" brukes i ekomloven § 2-7 femte ledd og i ekomforskriften § 7-1 første ledd. I forarbeidene til ekomloven beskrives trafikkdata som "data som angir kommunikasjonens opphavssted, bestemmelsessted, rute, klokkeslett, dato, omfang, varighet og underliggende tjeneste".[11] Begrepet dekker lagrede data om hvilke terminaler som har vært i bruk, ved hvilke basestasjoner[12] eller noder[13] trafikken starter og slutter, hvilken tjeneste som har vært i bruk (for eksempel samtale eller datatrafikk), dato og klokkeslett for når kommunikasjonen startet (som regel ned sekunders presisjon) samt omfang og varighet av for eksempel en samtale. Trafikkdata vil også omfatte unike identifikasjonsnummer som er i bruk ved kommunikasjonen, slik som telefonnummer, IP-adresse[14] mv.

Trafikkdata lagres hos de som eier og opererer kommunikasjonsnettverkene som kommunikasjonen går gjennom. Ved kommunikasjon i mobiltelefonnettet er det leverandørene av infrastrukturen som utgjør mobiltelefonnettverket som besitter dataene. Selv om det bare er noen få tilbydere som har infrastruktur (nettverk) for mobilkommunikasjon finnes det mange tilbydere av mobiltelefontjenester som ikke har egen infrastruktur. Kommunikasjon til og fra enhe-

[10] Sunde, I. M. (2006) "Lov og rett i cyberspace" s. 265.

[11] Ot.prp. nr. 58 (2002-2003) s. 92.

[12] En basestasjon er et anlegg som består av en eller flere antenner og sender- og mottakerutstyr for mobil telekommunikasjon. Mobilmasten er en byggkonstruksjon for å montere antenne. Sender- og mottakerutstyret står gjerne i et eget rom. Statens Strålevern (2016).

[13] En node er et knutepunkt på et nettverk som tar i mot datatraffik og sender den videre mot desitnasjonen.

[14] En IP-adresse (Internet Protocol) er en unik adresse som tildeles alle enheter som skal kommunisere i et TCP/IP basert nettverk, som for eksempel internett.

ter som er knyttet til disse tilbydernes tjenester vil gå i en av de etablerte mobilnettverkene og trafikkdata vil være lagret hos de som eier infrastrukturen.

Data om internettrafikk vil blant annet lagres hos leverandørene av internettjenester. Det er internettleverandørene som leverer ut internettmodem til sine kunder og de som har oversikt på hvilke IP-adresser deres kunder har fått tildelt.

Trafikkdata gir politiet relativt presise opplysninger om hvor personer kan ha vært til gitte tidspunkt. Selv om det ikke alltid gir nøyaktige plasseringer, vil det være en god pekepinn på om personen har vært der man mistenker at vedkommende var. Videre gir de informasjon om hvem som har vært i kontakt med hverandre, når og på hvilken måte (samtaler eller tekstmeldinger).

2.4 Betalingstransaksjoner

Finansavtaleloven § 12 bokstav a beskriver begrepet betalingstransaksjoner som en "handling som iverksettes av en betaler eller betalingsmottaker for å innbetale, overføre eller ta ut midler, uten hensyn til eventuelle underliggende forpliktelser mellom betaleren og betalingsmottakeren".

Data om betalingstransaksjoner er de data som lagres når disponeringer skjer på bankkontoer. Eksempler på dette kan være uttak i minibank, bruk av minibankkort i butikk, pengeoverføring, regningsbetaling mv. Disponeringene kan gjerne deles i to kategorier, uttak og betalinger. Det som kjennetegner et uttak er at data om transaksjonen bare sier noe om når og hvor uttaket har foregått, ikke hvem eller hva pengene har gått til. Betalinger kan være betaling av varer med kort, betaling med digitale bankløsninger (Vipps, mCash, MobilePay mv), overføring av penger i nettbank mv. Til forskjell fra uttak kan data om disse transaksjonene også vise hvem som har mottatt pengene.

Data om betalingstransaksjoner lagres av finansforetakene som forestår transaksjonen. Det kan være interne transaksjoner innenfor samme foretak eller transaksjoner mellom foretak. Betalingstransaksjoner vil vise hvilket beløp som er overført, hvilke kontoer beløpet er ført fra og til hvilket tidspunkt. Bruk av betalingskort vil vise hvilket kort som er brukt, hvem kortet tilhører, hvilken belastning (beløp) som er gjort og hvilken bankterminal som er brukt. Betalingstransaksjoner kan således si mye om personers kontakt med hverandre og disponeringer av penger mellom de og det kan si noe om personers bevegelser i forhold til bruk av bankkort i ulike minibanker og betalingsterminaler.

3 Utlevering av opplysninger etter personopplysningsloven

I vår digitale hverdag lagres det enorme mengder opplysninger som kan knyttes til oss som enkeltpersoner. Vår bruk av digitale enheter som mobiltelefoner, nettbrett og datamaskiner og i særlig grad disse enhetens kobling til internett, settes igjen mange spor. Det lagres informasjon om hvor vi er, hvilke applikasjoner vi bruker, hvilke søk vi gjør, hvilke nettsteder vi besøker og mer til. Stadig flere av tingene våre kobles til internett, slik som huset og bilen. Dette skjer samtidig med at kameraovervåkningen skjer i større grad med høyoppløselige kamera som kan vise små detaljer på relativt lang avstand. Alt dette setter personvernet på prøve samtidig som det genereres og lagres stadig flere potensielle bevis. Det er rimelig å anta at politiets ønske om å nyttiggjøre seg disse dataene som bevis i etterforskningen av straffesaker vil øke i årene fremover.

Personopplysninger vil utvilsomt kunne være til nytte for politiet i etterforskning av straffesaker så vel som ved søk etter savnede personer. Formålet med etterforskningen er å skaffe til veie de nødvendige opplysninger for å avklare det straffbare forhold og tjene til forberedelse for eventuell rettergang jf. strpl. § 226. Elektroniske spor som kan knyttes til bestemte personer vil være nødvendige opplysninger når disse kan bidra til å belyse saken. Opplysninger om mistenkte gjerningspersoner vil klart være nyttige for politiet men det vil i mange tilfeller også opplysninger knyttet til vitner og fornærmede også være. Når politiet ønsker tilgang til disse opplysningene må hensynet til personvernet og det offentliges behov veies mot hverandre.

3.1 Elektroniske spor som personopplysninger

Det må innledningsvis avklares om de aktuelle elektroniske spor er personopplysninger slik at behandling av opplysningene faller inn under personopplysningslovens regler. Personvernreglene kommer bare i betraktning i den grad de elektroniske sporene er personopplysninger,.

Personopplysninger er beskrevet i personopplysningsloven § 2 nr 1 som opplysninger og vurderinger som kan knyttes til en enkeltperson. I følge forarbeidene til personopplysningsloven er en ”enkeltperson” en person som direkte eller indirekte kan identifiseres, for eksempel ved hjelp av navn, identifikasjonsnummer eller et annet kjennetegn som er spesielt for personens fysiske, fysiologiske, psykiske, økonomiske, kulturelle eller sosiale identitet.[15] Ved vurdering av om en person lar seg identifisere, skal det tas i betraktning alle hjelpemidler som det er rimelig å tro at noen kan komme til å anvende for identifikasjonsformål og det vil dreie seg om en personopplysning selv om tilknytningen mellom personen og opplysningen bare er

[15] Ot.prp. nr. 92 (1998-1999) s. 102

kjent av noen få personer.[16] Det er ikke et krav at opplysningen lett skal kunne knyttes til en person, det er nok at muligheten er tilstede. Også krypterte opplysninger vil kunne være personopplysninger dersom der vil kunne være mulig for noen å gjøre opplysningene lesbare.

3.1.1 Kameraopptak

Det fremgår av personopplysningslovens § 3 første ledd jf. § 36 at kameraovervåking faller inn under personopplysningslovens regler og det gjelder uavhengig av om det tas opptak eller ikke. Personopplysningsloven § 36 definerer kameraovervåking som "vedvarende eller regelmessig gjentatt personovervåking ved hjelp av fjernbetjente eller automatisk virkende overvåkningskamera eller annet lignende utstyr som er fastmontert". Formålet med kameraovervåking er gjerne å overvåke noe på avstand og gjerne overvåke flere steder fra samme posisjon. Det kan både være områder der mennesker ferdes eller tekniske installasjoner som overvåkes og det er ikke all bruk av kameraovervåking som faller inn under personvernreglene. Det ene kriteriet er at det gjelder overvåking av personer. Begrepet "personovervåking" er ment å ha samme avgrensning som begrepet "personopplysning" har etter personopplysningsloven § 2-1.[17] Det vil si at kameraovervåkingen må være i stand til, eller i det minste potensiale til, å registrere bilder som kan brukes til å identifisere enkeltpersoner. For å vurdere som det er personovervåkning er det også tjenlig å se hen til formålet med overvåkningen. Hvis formålet er å overvåke tekniske installasjoner eller trafikkovervåking er det ikke personovervåking selv om individuelle kjennetegn i noen grad kan identifiseres.[18] Det andre kriteriet for at kameraovervåking faller inn under personvernreglene at overvåkingen er "vedvarende eller regelmessig". De enkeltstående eller mer tilfeldig gjentatte tilfeller av kameraovervåking vil falle utenfor definisjonen.[19]

3.1.2 Bompasseringsdata

Bakgrunnen for ordningen med innsamling av bompasseringsdata er å fakturere bilister for bruk av en gitt veistrekning som er delvis finansiert ved brukerbetaling. Teknologien med automatisk registrering har utviklet seg til dagens løsning med Autopass. Autopass er en løsning basert på en brikke som inneholder en unik identitet og som monteres på innsiden av frontruten. Informasjonen i brikken leses av når kjøretøyet som har brikken montert, passerer en automatisk bomstasjon.

Ved generering av bompasseringsdata lagres ikke opplysninger om personer, men registreringsnummer. Registreringsnummeret på et kjøretøy kan likevel brukes til å identifisere eier

[16] Ot.prp. nr. 92 (1998-1999) s. 102

[17] Johansen, M. W., Kaspersen, K., & Skullerud, Å. M. (2001) s. 259

[18] l.c.

[19] Johansen et.al. (2001) s. 260

av kjøretøyet. Disse opplysningene kan brukes til å nøste seg videre til en avklaring om hvem som var fører av kjøretøyet på det bestemte tidspunktet. Det skal ikke mer til enn å sende en tekstmelding som inneholder registreringsnummeret på et kjøretøy til et firesifret nummer for å få vite hvem som er registrert som eier på kjøretøyet. Det er således lett for en hver person å finne ut hvem som er eier av et gitt kjøretøy basert på registreringsnummeret. Personvernnemda har slått fast at Statens Vegvesens har adgang til å innhente bompasseringsdata fra de kjøretøy som ikke bruker Autopass-brikke med hjemmel i personopplysningsloven § 8 bokstav a.[20] I forbindelse med etablering av helautomatiske bomstasjoner har Datatilsynet gitt Statens Vegvesen konsesjon til behandling av personopplysninger knyttet til bompasseringer med hjemmel i personopplysningsloven § 33 andre ledd.[21]

3.1.3 Trafikkdata

Trafikkdata i den form oppgaven omhandler vil inneholde opplysninger som hvilket telefonnummer eller hvilken IP-adresse kommunikasjonen kommer fra og, i mange tilfeller, går til. Telefonnummer er en identifikator som lett kan knyttes til enkeltpersoner. Selv om man kan ha avtale med sitt telefonselskap om at sitt telefonnummer ikke skal fremkomme ved nummeropplysning, vil det være mulig i mange tilfeller å finne ut hvem som bruker et gitt telefonnummer. IP-adresser kan også brukes til å identifisere en abonnent. Det som kjennetegner telefonnummer, IP-adresser og andre identifikatorer i kommunikasjonsdata er at de er unike. Det som skiller en IP-adresse fra et telefonnummer er at en hel familie kan bruke samme IP-adresse for å komme på internett (fordi de kobler seg til internett med samme modem) og at IP-adresser ofte være dynamiske slik at abonnenten under gitte forutsetninger kan bli tildelt en ny og tilfeldig IP-adresse. Et telefonnummer vil være registrert på samme abonnent frem til denne aktivt sier opp abonnementet. Spørsmålet er i hvor stor grad man kan si at IP-adresser er egnet til å identifisere enkeltpersoner når alt fra enkeltpersoner til hele familier og bedrifter kan bruke samme IP-adresse på internett. Som personopplysninger kan IP-adresser sammenlignes med bompasseringsdata. Både IP-adresse og registreringsnummer kan knyttes til en konkret enhet (adresse eller kjøretøy), men både et kjøretøy og en internettilgang kan disponeres av mange forskjellige personer. Dag Wiese Schartum nevner problemstillingen i sine kommentarer til personopplysningsloven, uten at problemstillingen drøftes videre.[22] Det fremgår imidlertid av forarbeidene til Ekomloven[23] at reglene om behandling av personopplysninger i personopplysningsloven også gjelder for trafikkdata og konklusjonen er at trafikkdata generelt sett er å anse som personopplysninger, så vil det være opp til den behandlingsansvarlige å vurdere de tilfellene som faller utenfor.

---

[20] Personnemda (2005-11)

[21] Datatilsynet (2006)

[22] Schartum, D. W. (2000) s. 5

[23] Ot.prp. nr. 58 (2002-2003) s. 92

3.1.4 Betalingstransaksjoner

Data om betalingstransaksjoner vil inneholde informasjon om pengeoverføringer eller uttak av penger. Opplysningene vil kunne knyttes til en bestemt bankkonto og en bestemt bankkontoeier samt at de ved bruk av betalingskort også vil inneholde informasjon om hvilket kort som er brukt. Ved kontooverføringer og regningsbetalinger vil dataene også kunne inneholde to kontonummer og navn på to kontoeiere. Kontoeier kan være et foretak, og personopplysingsloven gjelder som utgangspunkt ikke for juridiske personer jf. personopplysningsloven § 2 nr 1. Betalingstransaksjoner som bare kan knyttes mellom foretak og ikke kan knyttes til en enkeltperson kan ikke regnes som personopplysninger. Det vil for eksempel være der et foretak har gjort en pengeoverføring til et annet foretak. Når det gjelder betalingstransaksjoner for øvrig er det ingen tvil om at det er opplysninger som kan knyttes til enkeltpersoner og at personvernreglene i utgangspunktet kommer til anvendelse.

3.1.4.1 Konklusjon

I kommentarutgave til personopplysningsloven nevnes fødselsnummer, bilnummer, telefonnummer og bankkontonummer som eksempler på opplysninger som kan knyttes til en enkeltperson.[24] Konklusjonen er at de elektroniske spor oppgaven omhandler som utgangspunkt er å anse som personopplysninger jf. personopplysningsloven § 2 nr 1. Oppgavens tema må derfor først og fremst drøftes under personvernreglene. Om noen tilfeller av kameraopptak, bompasseringsdata, trafikkdata og betalingstransaksjoner ikke faller inn under personopplysningslovens regler må de behandles direkte under de straffeprosessuelle regler.

3.2 Behandling av personopplysninger

Det er for så vidt ikke nok at en opplysning kan knyttes til en enkeltperson for å vernes av personvernreglene. Formålet med personopplysningsloven er å beskytte den enkelte mot krenking av personvernet ved behandling av personopplysninger, jf. § 1 første ledd. Opplysninger som ikke kan sies å krenke personvernet vil ikke falle inn under reglene.[25] Problemstillingen settes ikke på spissen her da de elektroniske spor som drøftes i oppgaven i alle tilfeller vil falle inn under formålet jf. drøftingen over.

Personopplysningsloven skal ivareta det grunnleggende personvernet og behovet for personlig integritet og privatlivets fred slik det er beskrevet i EMK art 8 ved å etablere regler for behandling av personopplysninger. Begrepet ”behandling av personopplysninger” omfatter all

[24] Johansen et.al. (2001) s. 68.

[25] ibid. s. 548.

formålstjent håndtering av personopplysninger.[26] Loven oppstiller at behandling er "enhver bruk av personopplysninger", herunder innsamling, registrering, sammenstilling, lagring og utlevering jf. § 2 nr 2. Lovens virkeområde er behandling som helt eller delvis foregår ved elektroniske hjelpemidler eller når de inngår i et personregister jf. § 3 første ledd bokstav a og b. Oppgavens tema berører elektronisk lagrede data og behandling av disse vil således være dekket av beskrivelsen. Det den enkelte gjør for personlige eller private formål ville falle utenfor lovens virkeområde jf. § 3 andre ledd.

Det er den som bestemmer formålet med behandlingen av personopplysningene som er behandlingsansvarlig for opplysningene jf. § 2 nr 4. Det betyr ikke nødvendigvis at det er denne som besitter dataene som er innsamlet, men oftest vil det nok være slik. Opplysningene kan også være lagret hos andre, som da er å anse som databehandler for opplysningene på vegne av den behandlingsansvarlige jf. § 2 nr 5. Jeg vil ikke sondre mellom disse begrepene da det er den behandlingsansvarlige som skal sørge for at behandlingen av opplysningene er i tråd med reglene, uavhengig av hvor de er lagret. Reglene i straffeprosessloven gjelder for den som "besitter" dataene, noe jeg vil komme tilbake til under kapittel 4.

Personopplysningsloven inneholder ikke regler om taushetsplikt, men regler for hvilken behandling av personopplysninger som er tillatt. Reglene vil minne om regler om taushetsplikt så langt det å dele opplysninger med andre ikke er en behandling som er tillatt etter loven. All behandling av personopplysninger krever hjemmel i lov. Utlevering av opplysninger er behandling og politiets tilgang til slike opplysninger for bruk i etterforskningen krever dermed at det foreligger hjemmel for det. Der det ikke er hjemmel i personopplysningsloven for å få utlevert opplysningene for bruk i etterforskningen, må man finne hjemmel andre steder. Grunnreglene for behandling av personopplysninger finner vi i personopplysingsloven § 11.

3.2.1 Grunnreglene for behandling av personopplysninger

Personopplysningslovens § 11 første ledd sier at personopplysninger bare kan behandles når det er tillatt etter § 8 og § 9 samt at opplysningene bare brukes til det som er formålet med behandlingen. Opplysningene kan videre ikke brukes til annet formål som er uforenlig med det opprinnelige formålet og den behandlingsansvarlige skal sørge for at opplysningene er tilstrekkelige og relevante for formålet samt korrekte og oppdaterte. Det er den behandlingsansvarliges plikt å sørge for at opplysningene slettes så snart det ikke lengre er nødvendig å lagre de ut i fra formålet. Reglene i § 11 første ledd er kumulative, det vil si at alle vilkår må være oppfylt for at behandlingen skal være lovlig. Det første kravet er, som nevnt, at person-

[26] Ot.prp. nr. 92 (1998-1999) s. 103.

opplysninger bare kan behandles når det er tillatt etter § 8 og § 9. Oppgaven begrenses til å bare drøfte personopplysninger under § 8, jf. avgrensingene i kapittel 1.4.

3.2.1.1 Personopplysningsloven § 8

3.2.1.1.1 Samtykke som grunnvilkår

Personopplysningsloven § 8 oppramser flere vilkår for å kunne behandle personopplysninger. Utgangspunktet er at behandling av personopplysninger fortrinnsvis skal være basert på samtykke fra den personen det registreres opplysninger om. I forarbeidene til personopplysningsloven sier departementet at behandling av personopplysninger i størst mulig grad bør basere seg på at den registrerte samtykker selv om det mulig å hjemle behandlingen i de andre grunnlagene som oppstilles i § 8.[27] Samtykke vil derfor være det foretrukne vilkår for behandling, selv om andre hjemler kan benyttes.

Et samtykke fra den registrerte til å behandle personopplysninger skal være "en frivillig, uttrykkelig og informert erklæring fra den registrerte om at han eller hun godtar behandling av opplysninger om seg selv" jf. § 2 nr 7. Samtykket må være klart og forståelig uttrykt og den som samtykker må ha fullstendig informasjon om hva vedkommende samtykker i. Det er ikke åpent for at "den som tier, samtykker" og kollektive samtykker gjennom tilknytning til en organisasjon eller lignende, fyller ikke kravene til samtykke etter reglene i § 2 nr 7.

3.2.1.1.2 Andre vilkår i personopplysningsloven § 8

En annen hjemmel for behandling etter § 8 er de tilfellene der det er fastsatt i lov at det er adgang til å behandle opplysningene. Der behandling av personopplysninger er fastsatt ved lov er det ikke noe krav til samtykke. Departementet sier i forarbeidene til personopplysningsloven at det ikke er noen grunn til å oppstille et tilleggsvilkår om samtykke for behandlingen når Stortinget allerede har bestemt at behandlingen er nødvendig. Rekkevidden av den enkelte lov som hjemler behandling av personopplysninger må tolkes på det konkrete tilfellet.[28]

Det neste alternativet i § 8 er at behandlingen er nødvendig etter ett eller flere av de vilkår som er satt i § 8 første ledd, bokstav a til f. Det som er felles for behandling etter vilkårene i bokstav a til f er at de er til dels skjønnsmessige kriterier. Det er den behandlingsansvarlige som må utvise dette skjønnet ved behandling av opplysninger, noe som i grensetilfeller kan være vanskelig. Datatilsynet har adgang til å overprøve skjønnet den behandlingsansvarlige utviser og kan både forlange at behandlingen opphører og kan veilede den behandlingsansvarlige slik at behandlingen blir lovlig. I forarbeidene påpeker departementet at det i noen tilfeller kan være vanskelige for den behandlingsansvarlige å gjøre disse vurderingene og konklu-

[27] Ot.prp. nr. 92 (1998-1999) s. 103.
[28] ibid. s. 109.

derer med at Datatilsynets praksis etter hvert vil trekke opp noen rammer for hvordan skjønnet skal utøves.[29]

3.2.1.2 Behandling for det uttrykkelig angitte formål

Som nevnt over er vilkårene i § 11 første ledd kumulative. Dermed er det ikke nok at behandlingen er dekket av et av vilkårene i § 8, de andre vilkårene i § 11 må også være oppfylt. Det neste kriteriet er at opplysningene bare skal brukes til det uttrykkelig angitte formål som kan saklig begrunnet i den behandlingsansvarliges virksomhet jf. § 11, første ledd bokstav b. Det gjelder all behandling, også innsamlingen og lagringen av opplysningene som skjer innledningsvis. Det er ikke åpent for å samle inn personopplysninger for andre formål en det som er nødvendig for at den behandlingsansvarlige skal kunne utføre sine oppgaver. I mange tilfeller, slik som ved lagring av kommunikasjonsdata og bompasseringsdata, vil behandling av opplysninger være nødvendig for å fakturere abonnenten for den faktiske bruk vedkommende har hatt til den pris som er avtalt. I slike tilfeller skal dataene slettes når det ikke lengre er nødvendig å lagre de for faktureringsformål, jf. § 28.

3.2.1.3 Behandling til annet formål

Det fremgår av § 11 første ledd bokstav c at de innsamlede opplysningene ikke kan brukes til et senere formål som er uforenelig med det opprinnelige formålet uten at den registrerte har samtykket til dette. Det kreves da et særskilt samtykke til en annen behandling enn den opplysningene er samlet inn for og man kan ikke støtte seg til samtykket som ble gitt innledningsvis. Selv om den opprinnelige innsamlingen ikke er basert på et samtykke, men for eksempel har hjemmel i lov, kan den registrerte samtykke i den nye behandlingen. I motsatt tilfelle, der den registrerte har samtykket i den opprinnelige behandlingen, og den nye behandlingen har hjemmel i lov, krever likevel gjenbruk av allerede innsamlede opplysninger et særskilt samtykke. Hvis samtykke ikke gis må opplysningene samles inn på nytt.

3.3 Utlevering til politiet

Den som har behandlingsansvaret for elektronisk lagrede data vil ofte være villig til å utlevere slike bevis til politiet for bruk i etterforskning av straffbare forhold. Spørsmålet er om den behandlingsansvarlige har kompetanse til å utlevere disse opplysningene under reglene om behandling av personopplysninger.

3.3.1 Særskilt om kameraovervåkning

Som nevnt over er kameraovervåkning særskilt beskrevet i personopplysningsloven kapittel 7. Opptak fra kameraovervåkning kan med hjemmel i § 39 siste punktum utleveres til politiet

[29] Ot.prp. nr. 92 (1998-1999) s. 109

ved etterforskning av straffbare handlinger eller ulykker så lenge ikke lovbestemt taushetsplikt er til hinder for det. Hvis opplysningene er underlagt lovbestemt taushetsplikt er det reglene om taushetsplikt i det enkelte tilfellet som bestemmer om utlevering kan skje. I slike tilfeller må reglene i om beslag og utleveringspålegg i straffeprosessloven nyttes.

Politiets bruk av opptak fra kameraovervåking vil i utgangspunktet være overskuddsinformasjon i forhold til det opprinnelige behovet, med mindre det opprinnelige behovet var å forebygge eller forhindre det samme straffbare forholdet som politiet etterforsker. Det er ikke oppstilt noe beviskrav i § 39, men der er rimelig å legge til grunn at beviskravet vil være det samme som etter reglene om beslag og utleveringspålegg, det vil si at opptaket må "antas å ha betydning som bevis" i den aktuelle straffesaken.

Utlevering av opptak fra kameraovervåking vil være behandling av personopplysninger etter § 11. Personopplysningsforskriften § 8-3 første ledd sier at bestemmelsen i § 11 første ledd bokstav c om at innsamlede opplysninger ikke kan brukes til annet formål uten den registrertes samtykke ikke er til hinder for at politiet bruker opptak fra kameraovervåking som de er i besittelse av i forbindelse med etterforskning av straffbare handlinger.

Konklusjonen er at ved etterforskning av straffbare forhold kan politiet få utlevert opptak fra kameraovervåking etter personopplysningsloven § 39 siste punktum og behandle disse med hjemmel i personopplysningsforskriften § 8-3. Reglene i personopplysningsloven gir ingen plikt for den behandlingsansvarlige til å utlevere opptak fra kameraovervåkning. Hvis den som besitter opptakene ikke ønsker å samarbeide med politiet, må veien gå om et utleveringspålegg etter straffeprosessloven § 210 første ledd. De straffeprosessuelle regler drøftes under kapittel 4.

3.3.2 Utlevering av opplysninger etter samtykke

Personvernreglene stenger for at personopplysninger kan brukes til annet formål en det opprinnelige uten samtykke fra den registrerte. Behandling av personopplysninger betinger at alle vilkårene i § 11 er oppfylt. Det betyr at en senere behandling av allerede innsamlede opplysningene med hjemmel i § 11 første ledd bokstav c, også må fylle de øvrige vilkårene i § 11 herunder være saklig begrunnet i den behandlingsansvarliges virksomhet. Likevel vil et samtykke alene være tilstrekkelig grunnlag for å utlevere opplysningene etter § 11 første ledd, bokstav c. Det fremkommer ikke direkte av loven, men det er beskrevet både i forarbeidene[30] og i kommentarutgaven[31] til personopplysningsloven. Av forarbeidene fremkommer det at i

[30] Ot.prp. nr. 92 (1998-1999) s. 114

[31] Johansen et.al. (2001) s. 118

de tilfellene gjenbruken er basert på et samtykke fra den registrerte vil ikke forenlighetskravet i § 11 første ledd bokstav b ha selvstendig verdi. Har den registrerte først samtykket i at opplysningene kan brukes til det nye formålet, som for eksempel kan være utlevering, vil dette være et tilstrekkelig grunnlag for behandlingen. Det har også fornuften ved seg at der den registrerte samtykker til utlevering (eller annen bruk) må det være unødvendig å måtte samle inn de allerede registrerte opplysningene på nytt.

For politiet er den enkleste måten å få utlevert lagrede data som er personopplysninger å få et samtykke fra den registrerte til at den behandlingsansvarlige kan utlevere de. Det vil i de fleste tilfeller være uproblematisk å få samtykke til å hente inn data når den registrerte er fornærmet i saken, for fornærmede vil som regel ha en interesse i å hjelpe politiet med å løse saken. Det vil selvfølgelig også forekomme at fornærmede ikke er samarbeidsvillig. Det kan være saker der fornærmede ikke ønsker å yte bistand fordi han eller hun selv har noe å skjule eller føler presset eller truet til å avstå fra samarbeid med politiet. Når det kommer til utlevering av data der den registrerte er vitne i saken kan det stille seg ulikt fra vitne til vitne og hvilken posisjon vitnet har. Vitner har ikke alltid en egeninteresse i at saken blir løst. Et vitne kan like gjerne være en venn av gjerningsmannen, og som helst ser at saken ikke løses. Siktede har ingen plikt til å medvirke i saken mot seg men kan likevel spørres om samtykke til å innhente elektroniske spor som kan brukes som bevis i saken.

Den behandlingsansvarlige kan være underlagt lovbestemt taushetsplikt i tillegg til behandlingsansvaret etter personopplysningsloven. Spørsmålet om disse reglene kommer i veien for utlevering av opplysninger til politiet når den registrerte samtykker, vil bli behandlet under kapittel 4.3.

3.3.3 Utlevering av opplysninger uten samtykke

Det vil være en del tilfeller der politiet ikke får innhentet samtykke til utlevering av personopplysninger. I noen saker vil politiet ha behov for å innhente opplysninger om alle kjøretøy som baserte en eller flere bestemte bompengestasjoner eller hvilke telefonnumre som har vært registret til en eller flere bestemte basestasjoner i et gitt tidsrom. Dette kan være aktuelt i mer alvorlige saker, som grove voldssaker, saker om seksuelle overgrep, ran, drap mv. Det vil i slike tilfeller ikke være mulig å identifisere de registrerte på forhånd og de vil dermed ikke få anledning til å gi et slikt samtykke selv om de kanskje ville gjort det.

En annen, og sikkert vanlig, problemstilling er når den registrerte ikke samtykker i utlevering. Det vil i mange tilfeller gjelde siktede, men kan som nevnt også gjelde andre involverte i saken. Det er ingen som har plikt til å samtykke til at opplysningene utleveres og spørsmålet er da om opplysningene kan utleveres uten samtykke. Som nevnt over i underkapittel 3.2.1.3 kan i utgangspunktet ikke opplysningene brukes til annet formål uten samtykke. Det betyr

ikke at enhver annen bruk betinger et uttrykt samtykke, men det stilles strenge krav til den nye behandlingen når samtykke ikke er gitt. Det skal blant annet være tett og nær sammenheng mellom det opprinnelige formålet og formålet med den nye behandlingen.[32]

Saker som omhandler utlevering etter personopplysningsloven har i liten grad vært behandlet i retten, men i Rt-2013-143 behandlet Høyesterett en sak som omhandler bruk av allerede innsamlede personopplysninger til et senere formål etter §11 første ledd bokstav c. Selv om saken ikke omhandler utlevering, så behandler Høyesterett vilkårene som gjelder for gjenbruk av allerede innsamlede opplysninger og saken er utvilsomt relevant for tolkningen av § 11 første ledd bokstav c.

Saken gjaldt et avfallshåndteringsselskap som hadde tatt i bruk et system med GPS-registrering for rapportering, administrasjon og drift av avfallstjenester. Systemet viste sjåførene veien til avfallsdunkene som skulle tømmes og sjåføren kvitterte for tømmingen eller en eventuell årsak til at dunken ikke ble tømt. Disse opplysningene ble registrert hos selskapet. Selskapet mottok tips om at deres kjøretøy sto parkert i lange perioder da de skulle vært i aktivitet i samme periode som noen av de ansatte hadde ført mye overtid. En samtale med en lærling på den ene bilen første til mistanke mot en konkret ansatt for føring av ureglementert overtid. Ledelsen i bedriften sammenstilte opplysningene generert av GPS-systemet med overtidslistene til den mistenkte ansatte for å avdekke overtidsføring som ikke var reell. Avfallsselskapet hevdet for retten at personopplysningsloven § 8 bokstav f ga hjemmel til den nye bruken av opplysningene. En av problemstillingene som retten måtte ta stilling til var om både personopplysningsloven § 8 bokstav f og § 11 første ledd bokstav c kunne gi hjemmel for gjenbruk av opplysninger til et annet formål enn det de er samlet inn til. Både tingretten og lagmannsretten la til grunn at bestemmelsene kunne være alternative hjemler til slik gjenbruk. Denne vurderingen hadde støtte i praksis blant annet i et vedtak fra personvernnemda.[33]

Førstvoterende mente at denne vurderingen ikke ga uttrykk for riktig rettsoppfatning da en slik tolkning ville innebære at bestemmelsen i §11 første ledd bokstav c får liten selvstendig betydning. Høyesterett påpeker at bestemmelsen i §11 første ledd bokstav c gir uttrykk for et formålsprinsipp om at innsamling av opplysninger skal skje til uttrykkelig angitte og saklige formål og at senere bruk ikke må være uforenelig med disse formål. Det støttes også av forarbeidene til personopplysningsloven at vilkåret i § 11 første ledd bokstav c vil utgjøre en viktig begrensning blant annet for å bruke elektroniske spor og til å samkjøre registre eller andre

[32] Ot.prp. nr. 92 (1998-1999) s. 114

[33] Personvernnemda (2004-3)

informasjonssamlinger.[34] Kravet til forenlighet innebærer at opplysningene ikke kan brukes til det nye formålet selv om det har hjemmel i § 8.

Dommen slår fast at gjenbruk av innsamlede opplysninger må både ha hjemmel i § 11 første ledd bokstav c og ett av alternativene i § 8. Det vil si at vilkårene i § 11 første ledd bokstav c utgjør et tilleggskrav til å bruke de innsamlede opplysningene til et annet formål enn det opprinnelige. Selv om bedriften ikke brukte opplysningene generert av GPS-systemet til en systematisk kontroll av de ansattes registreringer, kun til en enkeltstående kontroll basert på en konkret mistanke, konkluderte høyesterett med at den nye behandlingen var for fjernt avledet fra det opprinnelige formålet til at den var lovlig. I forarbeidene til personopplysningsloven oppgis kontrollformål som ett eksempel på formål som vil være uforenlig med det opprinnelige formålet, særlig når kontrollen ikke er en naturlig del av virksomheten til den behandlingsansvarlige, eller når ubehaget for den registrerte ikke står i rimelig forhold til fordelene av kontrollen.[35] Høyesteretts tolkning støttes også i juridisk litteratur.[36]

Det stadfestes i dommen at gjenbruk av allerede innsamlede opplysninger bare kan være lovlig når det er en saklig sammenheng mellom det opprinnelige formålet for innsamlingen og det nye formålet. Hvis det nye formålet er for fjernt avledet fra det opprinnelige, må det innhentes et særskilt samtykke til behandling. Utlevering av innsamlede opplysninger til politiet vil i de aller fleste tilfeller være for fjernt avledet fra det opprinnelige formålet til å være lovlig. Videre kan en utlevering av opplysninger til politiet til en viss grad sammenlignes med kontrollformål og det kan være ubehagelig for den registrerte at opplysningene brukes til etterforskning av straffbare forhold.

Konklusjonen er at reglene om behandling av personopplysninger ikke gir adgang for den behandlingsansvarlige til å utlevere opplysninger til politiet i de tilfellene der den registrerte ikke har gitt samtykke til dette. Unntak fra dette er opptak fra kameraovervåkning, jf. personopplysningsloven. § 39 siste punktum. Der den registrerte ikke har gitt sitt samtykke til utlevering er politiets henvist til å finne hjemmel i de straffeprosessuelle regler.

[34] Ot.prp. nr. 92 (1998-1999) s. 114

[35] l.c.

[36] Johansen et.al. (2001) s. 118 og Schartum, D. W. (2000) s. 8 - 9

4 Innhenting av elektroniske spor etter straffeprosessloven

Der reglene i personopplysningsloven ikke gir tilstrekkelig hjemmel for utlevering av elektroniske spor, henvises man til å løse problemstillingen under de straffeprosessuelle regler. Straffeprosesslovens fjerde del omhandler tvangsmidlene. Tvangsmidlene er ulike i art og det innebærer stor variasjon i hvor inngripende de ulike tvangsmidlene er. Like fullt er de tvangsmidler og det innebærer at bruken av det enkelte tvangsmiddel må vurderes opp i mot den generelle regel om forholdsmessighet i straffeprosessloven § 170a uavhengig av hvor lite inngripende tvangsmiddelet er. For det ene må et tvangsmiddel bare brukes når det er tilstrekkelig grunn til det. Kravet til tilstrekkelig grunn må ses opp i mot formålet med etterforskningen jf. strpl. § 226. For det andre må et tvangsmiddel bare brukes når det ikke etter sakens art og forholdende ellers anses som et uforholdsmessig inngrep. Ved vurdering om det er et uforholdsmessig inngrep må man vurdere inngrepets karakter, sakens alvor, alternative metoder for å oppnå formålet og hensynet til den inngrepet retter seg mot. Inngrep i borgernes rettssvære krever særskilt hjemmel i lov.[37] Det som kjennetegner elektroniske spor er at det er sjeldent mulig for politiet å komme til kunnskap om de samme opplysningene uten tilgang til lagrede data.

4.1 Innledende om beslag og utleveringspålegg

Straffeprosesslovens kapittel 16 omhandler de alminnelige, generelle regler om beslag og utleveringspålegg. Beslag og utleveringspålegg krever ikke at noen med skjellig grunn mistenkes for et straffbart forhold, men det er antatt i både rettspraksis og litteraturen[38] at det kreves skjellig grunn til å mistenke at et straffbart forhold er begått.. Utgangspunktet for at politiet kan ta gjenstander i beslag er at det er iverksatt etterforskning etter reglene i strpl. § 224 og formålet med beslaget må ses opp mot formålet med etterforskningens jf. § 226. Beslag i saken kan være ting som vil gi eller understøtte opplysninger i denne sammenheng. Det er ikke krav til en særskilt strafferamme for at en gjenstand kan tas i beslag, det kan gjøres i alle saker under etterforskning.

Straffeprosesslovens regler om beslag og utleveringspålegg vil generelt kunne være en hjemmel for utlevering av elektroniske spor til politiet. Beslag og utleveringspålegg kan være basert på en forutgående ransaking eller et sikringspålegg. Oppgaven vil først klargjøre de generelle reglene for beslag og utleveringspålegg og deretter hvordan de skal kommer til anvendelse i forhold til de konkrete elektroniske spor oppgaven handler om.

---

[37] NOU 2003:27 (2003) s. 44.

[38] se blant annet Andenæs, J., & Myhrer, T. (2009) s. 316, Bjerke, H. K., Keiserud, E. & Sæther, K.E. (2011) og Rt 1998 s. 1839.

4.1.1 Beslag

Beslag i gjenstander som kan ha betydning som bevis i straffesaker står som regel sentralt en etterforskning. Hovedregelen for beslag er å finne i straffeprosesslovens § 203. Det følger av etterforskningskompetansen i strpl. § 225 at det er politiet som tar beslag.

Politiet kan ta beslag i ting som antas å ha betydning som bevis. Beslag er en formløs prosess der politiet setter seg i besittelse av tingen som en del av etterforskningen. Det er ikke et krav at gjenstanden for beslag har en kjent eier eller at det tilhører en av partene i saken, men "betydning som bevis" må knyttes til en bestemt sak. Selv om bestemmelsen ligger under reglene om tvangsmidler, trenger ikke være fenomenet "tvang" være særlig fremtredende når det tas beslag. Det kan like gjerne være ting som frivillig overleveres til politiet som bevis i saken, for eksempel fra fornærmede.

Der beslagsbestemmelsen bruker ordet "ting" dekker begrepet alle fysiske ting, men det er sikker rett at også elektroniske spor omfattes av bestemmelsen.[39] I Rt 1992 s. 904 stadfester Høyesterett at "[…] også opplysninger som lagres på data og som i tilfellet må gjøres tilgjengelig ved utskrifter […]" faller inn under betegnelsen "ting". Bestemmelsen kan ses i sammenheng med bestemmelsen om sikringspålegg etter strpl. § 215a som sier at påtalemyndigheten kan gi pålegg om sikring av elektronisk lagrede data som antas å ha betydning som bevis.

Det fremgår av bestemmelsen at alle ting som "antas" å ha betydning som bevis, kan beslaglegges. Det stilles ikke høyere krav enn at man kan regne med at beviset vil å kaste lys over saken. En rimelig mulighet er nok og det kreves ikke så mye som skjellig grunn. Bevis vil være alt som kan kaste lys over spørsmålet om det er begått en straffbar handling, hvem som har begått handlingen,[40] hvordan den er begått, når og hvorfor forholdet har skjedd samt opplysninger som kan peke på uskyld og forhold som er relevante for skyldspørsmålet for øvrig.[41]

Det kan tas beslag i ting uavhengig av om besitteren har vitneplikt etter strpl. § 108. Det kan også tas beslag fra siktede, men det fremgår av strpl. § 204 første ledd at det ikke kan tas beslag i dokumenter og annet som et vitne kan nekte å forklare seg om etter reglene i strpl. §§ 117 – 121 og §§ 124 – 125 når tingen besittes av den som kan nekte å forklare seg eller av den som har rettslig interesse i hemmelighold. Eksempelvis kan det ikke tas beslag i legejournaler som er taushetsbelagt etter strpl. § 119 første ledd.

---

[39] Se Bjerke et.al. (2011) s. 711, Sunde (2006) 278 og Andenæs & Myhrer (2009) s. 317.

[40] Rt 1998 s. 1839.

[41] Bjerke et.al. (2011) s. 712.

Påtalemyndigheten beslutter beslag i ting som besitteren ikke vil utlevere frivillig jf. § 205. Den enkelte tjenestemann kan uten beslutning fra påtalemyndigheten ta beslag i forbindelse med pågripelse eller ransaking jf. § 206 første ledd. Det skal opptegnes skriftlig oversikt over det som beslaglegges og beslagene skal merkes.[42] Den som rammes av beslaget, kan kreve at spørsmålet om opprettholdelse av dette bringes inn for retten jf. § 208 første ledd.

Beslag etter strpl. § 203 betinger at politiet har direkte tilgang til tingen. Det kan skje ved at beslaget utleveres til politiet frivillig, at det utleveres etter beslutning som nevnt i § 205 eller at politiet blir i besittelse av beslaget i forbindelse med gjennomføring av pågripelse eller ransaking. Hvis politiet ikke har selvstendig tilgang til tingen må man gå veien om ransaking eller utleveringspålegg.

4.1.2 Om ransaking i databaser

Elektroniske spor av de kategoriene denne oppgaven har som tema er ikke opplysninger politiet på enkelt vis selv kommer i besittelse av. Dataene ligger lagret på servere hos de behandlingsansvarlige og det krever både tilgang til serverne og teknisk innsikt å få hentet de ut. En mulighet for politiet er å be retten om en beslutning til å ransake databasene med hjemmel i strpl. § 192 andre ledd nr 3 jf. 197 første ledd. Ved ransaking av datasystem kan enhver som har befatning med datasystemet pålegges å gi politiet nødvendige opplysninger for å få tilgang til systemet jf. § 199a. Slik bistand kan for eksempel være å gi politiet tilgangskoder til systemet. Bestemmelsen i § 199a sier ikke noe om at bistandsplikten skal omfatte å gi tilgang til innholdet i klar tekst. I forarbeidene til § 199a står det: ”Med tilgang til datasystemet menes også tilgang til data som er lagret i systemet”.[43] Om regelen kan tolkes til å gjelde for eksempel krypteringsnøkkel til krypterte data er usikkert.[44]

Om et slikt pålegg også omfatter en bistandsplikt til å hente ut de aktuelle dataene er tvilsomt. Det fremkommer i forarbeidene til § 199a at opplysningsplikten er begrenset til det som er nødvendig for å gi ”tilgang til” datasystemet.[45] Datakrimutvalget skriver i sin innstilling til implementering av Datakrimkonvensjonen at politiet ikke kan kreve at den som har bistandsplikt skal finne frem til konkrete opplysninger som politiet søker.[46] Bistand ut over å gi tilgang til datasystemet vil falle utenfor plikten etter strpl. § 199a men det stenger ikke for at noen som ønsker å bistå politiet, kan gjøre mer. Her må det skilles mellom ”rett” og ”plikt”.

[42] jf. strpl. § 207 første ledd og påtaleinstruksen § 9-5 første ledd
[43] Ot.prp. nr. 40 (2004-2005) s. 35
[44] Sunde (2006) s. 273.
[45] Ot.prp. nr. 40 (2004-2005) s. 35
[46] NOU 2003:27 (2003) s. 47

Så lenge opplysningene ikke er underlagt lovbestemt taushetsplikt kan den som har plikt til å gi politiet tilgang til systemet, også ha rett til bistå utover plikten. Det er en rimelig betraktning av så lenge man er fri til å avgi forklaring til politiet etter strpl. § 230 første ledd, kan man også gi politiet annen bistand. En ransaking av databaser for å finne data som kan beslaglegges vil kreve en del teknisk innsikt så lenge den som besitter dataene ikke er villig til å bistå frivillig. Da er det en enklere affære å pålegge besitteren å utlevere dataene.

4.1.3 Utleveringspålegg

Et utleveringspålegg etter straffeprosessloven § 210 første ledd kan brukes der politiet ikke har direkte og selvstendig tilgang til beviset. Reglene for utleveringspålegg går lengre enn reglene for beslag ved at den pålegget retter seg mot har en plikt til å aktivt utlevere beviset. Et annet skille mellom bestemmelsene er at beslag besluttes av påtalemyndigheten mens et utleveringspålegg besluttes av retten jf. § 210 første ledd. Det som kan være gjenstand for beslag etter strpl. § 203 vil også kunne være gjenstand for et utleveringspålegg. Det gjelder da blant annet elektronisk lagrede data. Det er besitteren som pålegges å utlevere beviset ved et utleveringspålegg.

Pålegg om utlevering av bevis er praktisk for politiet i de tilfellene der det ikke er grunn til å frykte at den pålegget retter seg mot vil destruere eller forringe beviset på annen måte. I motsatt fall vil beslag basert på en ransaking etter strpl. § 192 andre ledd være en bedre måte å sikre seg beviset på. Det kan videre være aktuelt å bruke utleveringspålegg der den som besitter tingen er villig til å samarbeide for å utlevere beviset, men vil at retten skal vurdere gyldigheten av politiets begjæring. Utleveringspålegg kan også være nyttig å bruke når man vet hvem som besitter tingen, men ikke hvor den er.[47]

Reglene om utleveringspålegg fanger opp Norges forpliktelser etter Datakrimkonvensjonen artikkel 18. Datakrimutvalget fastslo ved innføring av Datakrimkonvensjonen at § 210 allerede dekket forpliktelsene i artikkel 18 og at det ikke var behov for å foreslå noen lovendring ved innføring av denne artikkelen i konvensjonen.[48]

Et utleveringspålegg etter strpl. § 210 første ledd kan bare rettes mot den som har plikt til å vitne i saken. Vitneplikten gjelder for retten jf. § 108 og et utleveringspålegg kan ikke rettes mot den som har taushetsplikt etter reglene i strpl. §§ 117 flg med mindre taushetsplikten er opphevet, jf. blant annet § 118. Reglene om taushetsplikt i forhold til vitneplikt drøftes ytterligere under kapittel 4.3.

---

[47] Andenæs & Myhrer (2009) s. 324.

[48] NOU 2003:27 (2003) s. 42.

Et utleveringspålegg gis vanligvis som en formløs beslutning, men i praksis kan også formen kjennelse brukes. Regelen i strpl. § 210a om utsatt underretting av et utleveringspålegg etter § 210 gis ved kjennelse.

Påtalemyndigheten er gitt hastekompetanse etter § 210 andre ledd hvis det "ved opphold er fare for at etterforskningen vil lide". Når det gjelder elektroniske spor kan bestemmelsen ha en grensegang mot sikringspålegg etter strpl. § 215a, som drøftes nedenfor. Påtalemyndighetens beslutning skal snarest fremlegges for retten etter § 210 andre ledd andre punktum. Beslutningen etter andre ledd skal som fortrinnsvis være skriftlig og skal inneholde formålet med pålegget og hva det omhandler jf. § 210 fjerde ledd, jf. §197 tredje ledd.

4.1.4 Sikringspålegg

Bestemmelsen om sikringspålegg i straffeprosesslovens § 215a kom inn ved lovendring i 2005.[49] Hensikten med bestemmelsen er å gi politiet hurtig tilgang til sikring av elektroniske data som ellers kan bli tapt. Et sikringspålegg gir ikke politiet tilgang til dataene, men pålegger besitteren å sikre de på en måte som ivaretar dataenes integritet, tilgjengelighet og autentisitet.[50]

Det er Påtalemyndigheten som beslutter et sikringspålegg og det stilles samme beviskrav til et pålegg om sikring av data som ved beslag etter strpl. § 203. Bestemmelsen gjelder alle typer data så lenge de er elektronisk lagret og omfatter både trafikkdata og innholdsdata.

Elektroniske data som er sikret etter § 215a kan bare utleveres etter reglene i straffeprosessloven § 210. Det fremkommer ikke av ordlyden i bestemmelsen, men er klart forutsatt i forarbeidene der det står: "Data som er sikret gjennom et sikringspålegg, kan i utgangspunktet bare kreves utlevert innenfor rammen av straffeprosesslovens § 210".[51]

4.1.5 Beslag basert på utleveringspålegg

Det er naturlig å se bestemmelsene om beslag og utleveringspålegg i sammenheng med tanke på at "ting" som tilkommer politiet ved et utleveringspålegg også er gjenstand for beslag etter § 203. Det fremkommer av § 203 at beslaget kan gjelde inntil rettskraftig dom foreligger i saken, og det samme vil gjelde for bevis som er utlevert etter § 210. Bestemmelsen om beslag sier ikke noe om hvordan tingen kommer i politiets besittelse og bestemmelsene om opphevning av beslaget i § 213 og tilbakelevering i § 214 gjelder uavhengig av om beslaget er til-

[49] Endret ved Lov 8 april 2005 nr. 16.
[50] Ot.prp. nr. 40 (2004-2005) s. 7 og s. 36.
[51] Ot.prp. nr. 40 (2004-2005) s. 29

kommet ved et utleveringspålegg eller på annen måte. Kravet til opptegning av beslaget[52] tilsier at også ting som er utlevert til politiet basert på et utleveringspålegg må anses som beslag. Det kreves imidlertid ingen beslutning fra påtalemyndigheten for å opprettholde beslag på bakgrunn av utleveringspålegg fordi retten har allerede besluttet beslaget. I forarbeidene til gjennomføring av Datalagringskonvensjonen i norsk rett i omtales elektroniske spor som beslag uansett om det er tatt beslag dataene etter strpl. § 203 eller de er utlevert etter § 210.[53]

4.2 Utlevering når besitteren har vitneplikt

Reglene i straffeprosessloven reiser flere problemstillinger i forhold til politiets tilgang til elektroniske spor under etterforskningen. Den første problemstillingen er om dem som besitter opplysningene frivillig kan utlevere disse når det ikke foreligger samtykke. Det er drøftet og konkludert over at det ikke er mulig under personopplysningslovens regler. Den neste problemstillingen er da i hvilken grad de straffeprosessuelle reglene åpner for utlevering av opplysninger når den registrerte ikke har samtykket i utleveringen.

Reglene om beslag og utleveringspålegg i straffeprosessloven må ses i sammenheng med reglene om vitneplikt etter strpl. §§ 108 flg. Som nevnt over kan beslag tas uavhengig av om besitteren har vitneplikt[54] mens et utleveringspålegg kun kan rettes mot den som har vitneplikt i saken. Hvis den som er i besittelse av lagrede data som er underlagt lovbestemt taushetsplikt etter strpl. §§ 117 flg utleverer disse til politiet uten at taushetsplikten er opphevet, vil det være et brudd på straffebestemmelsen i strl. § 209 første ledd. Den som har vitneplikt kan også pålegges å legge frem dokumenter som han har plikt til å forklare seg om jf. strpl. § 116 første ledd og det gjelder uavhengig av om den opplysningene gjelder ikke ønsker at politiet kommer til kjennskap om opplysningene. Vitneplikten etter strpl. § 108 gjelder bare for retten. Straffeprosessloven § 230 første ledd første setning sier at ingen har plikt til å forklare seg for politiet med unntak av noen tilfeller nevnt i § 230 første ledd andre setning og andre ledd. Politiet har likevel anledning til å ta opp forklaring av mistenkte, vitner og sakkyndige som ønsker å avgi slik forklaring. Den som har vitneplikt for retten og som ønsker å avgi vitneforklaring til politiet, vil også kunne frivillig utlevere opplysninger til politiet som han ellers ville blitt pålagt å forklare seg om i retten. Vitnepliktens skranker er til en viss grad sammenlignbare med forutsetningene for å ta beslag. Det kreves at etterforskning av konkrete forhold er igangsatt, men ikke at det er en bestemt mistenkt for forholdet.[55]

[52] jf. strpl. § 207 og påtaleinstruksen § 9-5 første ledd

[53] Prop.49L (2010-2011) s. 93

[54] med unntak av begrensningene i strpl. § 204 første ledd

[55] Andenæs & Myhrer (2009) s. 192

I forbindelse med behandling av datalagringsdirektivet skriver departementet at "Dersom taushetsplikten oppheves med hjemmel i straffeprosessloven § 118 første ledd, er det formelt ikke noe til hinder for at tilbyder frivillig utleverer trafikkdata.".[56] Det samme vil også gjelde andre bevis som er underlagt vitneplikt.

Konklusjonen er at den som besitter lagrede data som politiet ønsker utlevert og som besitteren har vitneplikt om etter strpl. § 108, kan frivillig utlevere disse dataene til politiet selv om den registrerte ikke samtykker og politiet kan ta dataene i beslag.

4.2.1 Utlevering av bompasseringsdata

Den som har behandlingsansvar for bompasseringsdata har vitneplikt etter strpl. § 108 da bompasseringsdata ikke er underlagt lovbestemt taushetsplikt. Den som besitter dataene kan utlevere dataene til politiet basert på vitneplikten, jf. drøfting over. Det kan likevel forekomme at besitteren vil be om en beslutning om beslag fra påtalemyndigheten. Politiet må fremme en begjæring om å få konkrete opplysninger om bompasseringer utlevert som bevis til den pågående etterforskning. I de tilfellene besitteren av bompasseringsdataene ikke ønsker å samarbeide med politiet om utlevering eller ønsker rettens vurdering av beslaget, kan politiet be retten om å utferdige et utleveringspålegg jf. strpl. § 210 første ledd.

Som nevnt over er det retten som beslutter et utleveringspålegg men påtalemyndigheten er gitt hastekompetanse der det er fare for at etterforskningen ellers vil lide. Bompasseringsdata lagres i utgangspunktet i 5 år etter dagens bokføringsregelverk.[57] Det finnes imidlertid såkalt "sporfri avtale" der dataene slettes fortløpende. Ved en slik sporfri avtale slettes passeringsdataene så snart de er avregnet mot avtalen.[58] For å ha mulighet til å sikre slike data, må de sikres før passeringen belastes avtalen. I slike tilfeller vil det være aktuelt for påtalemyndigheten å bruke hastekompetansen etter strpl. § 210 andre ledd.

Et utleveringspålegg etter straffeprosessloven § 210 betinger at de aktuelle dataene kan identifiseres. Det kan ikke gis pålegg om å utlevere alle tilgjengelige data.[59] Hvis politiet ikke vet hvilke data de er ute etter må veien gå om ransaking. Når det gjelder innhenting av bompasseringsdata vil dette neppe by på problemer, da det er mulig å både identifisere hvor dataene er og konkretisere hvilke data politiet vil pålegge utlevert. En begjæring om et utleveringspålegg til retten bør inneholde en konkret oversikt over hvilke data som ønsker utlevert, dvs hvilke registreringsnummer og hvilke bompengeanlegg det skal sikres data fra og en begrunnet over-

[56] Prop. 49L (2010-2011) s. 95.
[57] Statens Vegvesen (2017).
[58] Fjellinjen (2015).
[59] Andenæs & Myhrer (2009) s. 324.

sikt over hvilken tidsperiode utleveringspålegget skal omfatte. Utleveringspålegget legges så frem for den som besitter dataene for å få disse utlevert. Hvis den som besitter dataene bestrider grunnlaget for utleveringspålegget, kan beslutningen ankes jf. strpl. § 377 første ledd, men hvis besitteren nekter å etterkomme ett rettskraftig utleveringspålegg kan det ilegges rettergangsbot etter domstolsloven § 206 første ledd. Straffeprosessloven regler om beslag og utleveringspålegg retter seg mot den som besitter dataene uavhengig av hvilken rolle besitteren har i forhold til reglene i personopplysningsloven. Det kan være den behandlingsansvarlige, men det kan også være en annen som er databehandler på vegne av den som har behandlingsansvaret.

Konklusjonen er at bompasseringsdata er personopplysninger som ikke er underlagt lovbestemt taushetsplikt og at slike opplysninger kan utleveres til politiet frivillig av besitteren selv om den registrerte ikke har samtykket i utleveringen. I de tilfellene der den behandlingsansvarlige ikke ønsker å utlevere opplysningene frivillig må politiet be retten om et utleveringspålegg rettet mot den som besitter dataene.

4.3 Utlevering når besitteren har taushetsplikt

Et utleveringspålegg kan bare rettes mot den som har vitneplikt i saken. I flere tilfeller er elektronisk lagrede data underlagt taushetsplikt. Det finnes mange former for taushetsplikt, både avtalefestet og lovbestemt taushetsplikt. Jeg vil ta for meg reglene om taushetsplikt som gjelder for de kategorier av elektroniske spor som oppgaven omhandler. Kameraovervåkning og bompasseringsdata er allerede drøftet i oppgaven, for det er normalt ikke opplysninger som er underlagt lovbestemt taushetsplikt. Betalingstransaksjoner og trafikkdata er derimot opplysninger som er underlagt lovbestemt taushetsplikt, men de er underlagt forskjellige regelsett og vil drøftes hver for seg.

Vitneplikten etter strpl. § 108 gjelder ”enhver” som etter innkalling plikter å forklare seg for retten med mindre annet er bestemt i lov. Vitneplikten er dermed ikke absolutt og unntakene kan deles i de tilfeller der enkelte vitner kan velge å påberope seg fritak for vitneplikt jf. strpl. §§ 122 - 125 og de tilfeller som nekter retten å ta imot forklaring jf. strpl. §§ 117 – 121. De former for lovbestemt taushetsplikt som ikke viker for vitneplikten etter strpl. § 108 faller under den siste kategorien. Den lovbestemte taushetsplikt gjelder ikke ubetinget. Den gjelder bare det vedkommende har fått vite ”i sitt virke”. Hvis for eksempel en lege har vært vitne til et innbrudd gjelder ikke taushetsplikten etter strpl. § 119 første ledd om det han har observert. Taushetsplikten gjelder kun de opplysningene legen får i sitt virke som lege. Videre gjelder taushetsplikten beskyttelsesverdig informasjon. At pasientopplysninger er underlagt taushetsplikten er klart, men hvor legen jobber eller om han var på jobb en bestemt dag er ikke beskyttelsesverdige opplysninger. Et annet unntak fra taushetsplikten er der opplysningene er nødvendige for å hindre at en uskyldig blir straffet jf. strpl. § 119 tredje ledd.

4.3.1 Utlevering av data om betalingstransaksjoner

Opplysninger om betalingstransaksjoner er underlagt taushetsplikt etter finansforetaksloven § 9-6 og § 16-2. Finansforetaksloven kom i 2015 og erstattet sparebankloven, forretningsbankloven og finansieringsvirksomhetsloven. Ansatte og tillitsvalgte i finansforetak har taushetsplikt om opplysninger de får kjennskap til gjennom sitt virke om kunders og andres forretningsmessige eller personlige forhold etter § 9-6 første ledd. Videre har foretaket en selvstendig taushetsplikt for sine kunders og andres forretningsmessige eller personlige forhold etter § 16-2 første ledd. Taushetsplikten gjelder "forretningsmessige eller personlige forhold" og for å avklare om det omfatter betalingstransaksjoner må begrepet tolkes. Begrepet er ikke beskrevet i forarbeidene til loven så det må ses hen til andre kilder. Bjørn Engstrøm gjør rede for forsikringsselskapers taushetsplikt etter forsikringsvirksomhetsloven i tidsskrift for forretningsjus.[60] I redegjørelsen presiseres det at opplysninger om alle sider ved et kundeforhold er underlagt taushetsplikt. Det gjelder både personlige, økonomiske og forretningsmessige forhold. Under personlige forhold faller helseopplysninger, familiære forhold og privatøkonomiske forhold.[61] Betalingstransaksjoner omhandler helt klart privatøkonomiske forhold, da de kan vise innskudd, uttak og betalinger både med kort og fakturabetalinger. Det er rimelig å legge til grunn en tilvarende tolkning av bestemmelsene om taushetsplikt i finansforetaksloven som det er gjort under forsikringsvirksomhetsloven. Sistnevnte lov er avledet av reglene i tidligere finansieringsvirksomhetsloven som ble erstattet av finansforetaksloven i 2015. Ved en slik tolkning vil reglene om taushetsplikt etter finansforetakslovens § 9-6 første ledd og § 16-2 første ledd gjelde data om betalingstransaksjoner.

Den lovbestemte taushetsplikten etter tidligere sparebankloven, forretningsbankloven og finansieringsforetaksloven gjaldt ikke forklaring for retten og utlevering av opplysninger var hjemlet i den generelle regelen om utleveringspålegg i strpl. § 210 første ledd. De ansatte hadde, som andre vitner, ingen plikt til å forklare seg for eller utlevere opplysninger til politiet. Ved en lovendring i 2004[62] kom det nye regler i straffeprosessloven om at ansatte ved blant annet finansinstitusjoner har forklarings- og utleveringsplikt for politiet om de forhold som ellers er underlagt den lovpålagte taushetsplikten. Forklaringsplikten ble lagt til i et nytt andre ledd i strpl. § 230 mens utleveringsplikten ble lagt til i et nytt tredje ledd til strpl. § 210.

[60] Engstrøm (2004).

[61] ibid. s. 4.

[62] Lov av 25 juni 2004 nr. 52.

Den som har taushetsplikt etter reglene i finansforetaksloven plikter etter straffeprosessloven § 230 andre ledd å avgi forklaring til politiet om forhold som omfattes av taushetsplikten.[63] Straffeprosesslovens § 210 tredje ledd sier at de som har forklaringsplikt etter § 230 andre ledd også plikter å utlevere dokumenter og annet som antas å ha betydning som bevis og som omfattes av den samme forklaringsplikten. Utleveringsplikten etter straffeprosesslovens § 210 tredje ledd gjelder de samme "ting" som første ledd[64] og elektronisk lagrede data er dermed omfattet av beskrivelsen.

Det fremkommer av bestemmelsene både i strpl. § 230 andre ledd og § 210 tredje ledd at plikten gjelder ved etterforskning av straffbare forhold. Det er tatt inn et alternativ om at plikten også kan gjelde andre forhold når "sterke allmenne hensyn" tilsier det. Disse tilfellen drøftes ikke da oppgaven omhandler saker under etterforskning, men et typisk tilfelle som nevnes i forarbeidene er i forsvinningssaker der det er behov for å forsøke å finne ut hvor den forsvunne befinner seg.[65]

Konklusjonen er at finansforetak og deres ansatte (og tillitsvalgte) med hjemmel i straffeprosessloven § 210 tredje ledd jf. § 230 andre ledd plikter å utlevere data om betalingstransaksjoner uten den registrertes samtykke og uavhengig av den lovbestemte taushetsplikt.

4.3.2 Utlevering av trafikkdata

Tilbydere av elektroniske kommunikasjonstjenester har taushetsplikt etter ekomloven § 2-9 første ledd. Dette også gjelder andre som utfører arbeid for tilbyderen jf. andre ledd. Ekomforskriften § 7-1 presiserer videre at "Tilbyder skal bevare taushet om trafikkdata etter ekoml § 2-9, og skal slette eller anonymisere trafikkdata etter ekoml § 2-7 tredje ledd".

Tilbyder av elektronisk kommunikasjonstjeneste har ikke særskilt forklarings- og utleveringsplikt for politiet, slik ansatte i finansforetak har. Der er da den alminnelige vitneplikten for retten etter strpl. § 108 som gjelder. Taushetsplikten etter ekomloven viker derimot ikke for vitneplikten etter strpl. § 108. Det fremkommer av straffeprosessloven § 118 første ledd som blant annet sier at "Uten samtykke fra departementet må retten ikke ta imot forklaring som vitnet ikke kan gi uten å krenke lovbestemt taushetsplikt han har fått som følge av tjeneste

[63] I bestemmelsen står det at forklaringsplikten gjelder den som har taushetsplikt etter blant annet sparebankloven § 21, forretningsbankloven § 18 og finansieringsvirksomhetsloven § 3-14 men etter oppheving disse lovene ble det lagt inn en henvisning til finansforetaksloven som dekker den samme taushetsplikten.

[64] Bjerke et.al. (2011) s. 726

[65] Se Ot.prp. nr. 59 (2003-2004) s. 54 og Bjerke et.al. (2011) s. 727

eller arbeid for stat eller kommune". Det er i særlig grad de som taushetsplikt etter forvaltningsloven §§ 13 flg retten ikke kan ta imot forklaring fra.[66]

Tidligere var det bare Televerket som befattet seg med elektroniske kommunikasjonstjenester, slik som telefontjenester. Televerket var en offentlig etat og de ansatte hadde status som offentlig ansatte. Ved omdanning av Televerket til aksjeselskap ble det gjort en tilføyelse i strpl. § 118 første ledd slik at taushetsplikten også gjaldt den gjorde tjeneste eller arbeid for "teleoperatør".[67] Da ekomloven kom i 2003 ble beskrivelsen i § 118 første ledd tilpasset slik at den var i overenstemmelse med beskrivelsen som ble brukt i ekomloven. Dagens bestemmelse sier at "Tilsvarende gjelder for vitne som har taushetsplikt som følge av tjeneste eller arbeid for […] tilbyder av tilgang til elektronisk kommunikasjonsnett eller elektronisk kommunikasjonstjeneste, elektronisk kommunikasjonsinstallatør […]". Det betyr at de som har taushetsplikt etter ekomloven § 2-9 første ledd er de samme personene retten ikke kan oppta forklaring av etter straffeprosessloven § 118 første ledd, andre punktum, tredje alternativ.

Reglene om beslag og utleveringspålegg er begrenset av reglene om vitneplikt med den følge at taushetsplikten etter ekomloven stenger både for beslag og utleveringspålegg. Selv om det i utgangspunktet kan tas beslag hos den som ikke har vitneplikt i saken kan det etter reglene i , strpl. § 204 ikke tas beslag i dokument eller annet som et vitne ikke kan forklare seg om etter bestemmelsene i §§ 117-121 og §§ 124-125. Med "dokument eller annet" vil også datafiler omfattes.[68] Trafikkdata vil utleveres som datafiler og beslagsforbudet i strpl. § 204 første ledd vil også gjelde disse. Regelen gjelder for beslag som besittes av den som kan nekte å forklare seg eller av den som har rettslig interesse i hemmelighold. Tilfellet med trafikkdata er at de besittes av den som ikke kan forklare seg. Regelen kan ses i sammenheng med regelen om utleveringspålegg. Kun den som har vitneplikt i saken kan pålegges å utlevere bevis etter § 210. Utleveringspålegg nyttes der politiet ikke har en selvstendig og direkte tilgang til beviset. Hvis politiet skulle ha selvstendig tilgang til datafiler som er taushetsbelagt etter reglene i straffeprosessloven § 118 første ledd, jf. Ekomloven § 2-9 første ledd, kan det likevel ikke tas beslag i disse på grunn av begrensningen i strpl. § 204 første ledd.

Det fremgår av straffeprosessloven § 118 første ledd, første setning at det "uten samtykke fra departementet" ikke kan tas opp forklaring om opplysninger som er underlagt taushetsplikt. Departementet kan samtykke til at forklaring gis om ellers taushetsbelagte opplysninger. Det kan ikke gis samtykke til å oppheve taushetsplikten for alle opplysninger som er taushetsbelagte. Det må gjelde de nærmere angitte opplysninger som politiet mener vil ha betydning

[66] Bjerke et.al. (2011) s. 451.

[67] Endret ved Lov 24 juni 1994 nr. 45.

[68] Andenæs & Myhrer (2009) s. 319.

som bevis i den konkrete sak. Bestemmelsens første ledd, siste bokstav sier at slikt samtykke bare kan nektes om åpenbaringen vil utsette staten eller allmenne interesser for skade eller virke urimelig overfor den som har krav på hemmelighold. Kompetansen departementet har til å oppheve taushetsplikten kan delegeres og for trafikkdata har Samferdselsdepartementet delegert denne kompetansen til Nasjonal Kommunikasjonsmyndighet.

Før samtykke gis må det gjøres en selvstendig og konkret vurdering av at ikke statens eller allmenne interesser utsettes for skade eller at det virker urimelig for den som har krav på hemmelighold. Det er departementet eller som har delegert kompetanse som må gjøre denne vurderingen. Det er da Nasjonal Kommunikasjonsmyndighet som behandler anmodninger om å oppheve taushetsplikten for trafikkdata. Ved innhenting av trafikkdata knyttet til enkelte telefonnummer eller IP-adresser vil sjelden staten eller de allmenne interesser utsettes for skade. De fleste tilfeller som må vurderes vil gjelde hensynet til den som har krav på hemmelighold. De allmenne interessert kan imidlertid stenge for muligheten til å innhente store mengder data basert på hvilke basestasjoner som har vært i bruk. I slike tilfeller kan politiet få tilgang til mye kommunikasjonsdata som ikke tilhører noen som er knyttet til saken.

Under taushetsplikten etter ekomloven § 2-9 første ledd vil "Den som har krav på hemmelighold" være brukeren eller abonnenten av den aktuelle kommunikasjonstjenesten. Hensynet til vitnet som har taushetsplikt er irrelevant, noe som også fremkommer av forarbeidene til straffeprosessloven.[69] Det er kun hensynet til de offentlige eller allmenne interesser eller hensynet til den som har krav på hemmelighold som skal vurderes.

Departementet v/Nasjonal Kommunikasjonsmyndighet må gjøre en urimelighetsvurdering i forhold til om samtykke til å oppheve taushetsplikten for tilbyderen kan gis. Ved denne urimelighetsvurderingen må hensynet til kriminalitetsbekjempelse settes opp mot personvernhensynene. Begrepet "urimelig" viser til at det må tas noe hensyn til den som er vernet av taushetsplikten, men at skrankene ikke skal være veldig høye. En sentralt moment ved vurderingen vil være sakens art og alvorlighet. Det vil rimeligvis være lettere å oppnå at taushetsplikten oppheves i alvorlige saker enn ved de mer bagatellmessige forhold. Det skal nok likevel ikke så alvorlige saker til før Nasjonal Kommunikasjonsmyndighet vil oppheve taushetsplikten for tilbyderne når det kan argumenteres for at opplysningene vil ha betydning som bevis. I 2009 behandlet forgjengeren til Nasjonal Kommunikasjonsmyndighet, Post- og Teletilsynet, 2 015 begjæringer om fritak fra taushetsplikt etter ekomloven § 2-9 første ledd og i 89 % av sakene ble taushetsplikten opphevet.[70]

[69] Ot.prp. nr. 35 (1978-1979) s. 142
[70] Prop. 49L (2010-2011 s. 46

Det fremkommer av forarbeidene til straffeprosessloven at det under urimelighetsvurderingen må legges vekt på hvor vesentlig vitnemålet er for saken og hvordan muligheten er for å føre beviset på annen måte.[71] Det vil i de fleste tilfeller være vanskelig å underbygge opplysningene på en tilsvarende god måte uten å få utlevert trafikkdata. Det er klart at mange av de opplysningene man får fra trafikkdata, vil man også kunne få hvis man kan sikre innholdsdata fra de mobiltelefonene som er brukt i kommunikasjonen. Utfordringene derimot, er for det ene å få tak i disse telefonene, og det andre er at det kan tidvis være vanskelig å sikre innhold fra moderne telefoner uten samarbeid fra den som bruker telefonen, blant annet grunnet kryptering av innholdet mv. Forklaring om de samme opplysningene som trafikkdata vil gi, vil sjelden være særlig presise og troverdigheten er vanskeligere å etterprøve. I undersøkelsen om innhenting av trafikkdata som er nevnt over svarte 26 % av respondentene at "trafikkdata var ressursbesparende for saken ved at andre metoder/undersøkelsen kunne utelates".[72]

Et annet moment ved vurderingen som skal gjøres før taushetsplikten kan oppheves er hva slags opplysninger taushetsplikten omfatter, for eksempel om det er strengt personlige eller økonomiske opplysninger.[73] Opplysninger fra trafikkdata vil sjelden falle i kategorien "strengt personlige eller økonomiske opplysninger" da det er statiske opplysninger om kommunikasjon som har foregått i kommunikasjonsnettverket og ikke innhold fra kommunikasjonen som vil fremkomme av dataene.

I og med at beslag og utleveringspålegg er tvangsmidler må det ikke anses som et uforholdsmessig inngrep å gjennomføre tvangsmiddelet jf. § strpl. 170a. Denne uforholdsmessighetsvurderingen vil i stor grad overlappe med urimelighetsvurderingen etter § 118 første ledd, tredje punktum. Urimelighetsvurderingen etter § 118 gjøres av Nasjonal Kommunikasjonsmyndighet under behandling av anmodning om å oppheve taushetsplikten mens uforholdsmessighetsvurderingen etter § 170a gjøres av påtalemyndigheten ved beslag og av retten ved beslutning om utleveringspålegg.

Retten er gitt kompetanse til å overprøve vedtak etter strpl. § 118 første ledd, enten samtykke er gitt eller nektet jf. strpl. § 118 andre ledd. Spørsmålet kan bringes til retten av partene. Det kan både være politiet som vil prøve gyldigheten av et nektet samtykke eller det kan være tilbyderen som vil prøve gyldigheten av et gitt samtykke. Hvis spørsmålet om gyldigheten av en avgjørelse fra departementet fremmes, må retten gjøre en avveining mellom hensynet til taushetsplikten og hensynet til sakens opplysning og departementet skal gis anledning til å

[71] Ot.prp. nr. 35 (1978-1979) s. 142.
[72] Prop. 49L. (2010-2011) s. 49.
[73] Bjerke et.al. (2011) s. 457.

redegjøre for sitt standpunkt før retten fatter sin avgjørelse. Rettens avgjørelse gis ved kjennelse og kan påankes jf. strpl. § 377 første ledd.

Den som har krav på hemmelighold etter § 118 første ledd siste punktum kan ikke fremme sak for retten om å overprøve et vedtak om å oppheve taushetsplikten. I de tilfellene der Nasjonal Kommunikasjonsmyndighet har opphevet taushetsplikten for en tilbyder av kommunikasjonstjenester, er det den aktuelle tilbyderen som kan bringe spørsmålet for retten.

Et samtykke fra den registrerte vil ha samme virkning under reglene i straffeprosessloven som under reglene i personopplysningsloven. Hvis den som har krav på hemmelighold samtykker til at opplysningene kan utleveres, faller taushetsplikten bort.[74] Det fremkommer blant annet av ekomloven § 2-7 femte ledd og ekomforskriften § 7-1 fjerde ledd.

I alle tilfeller der taushetsplikten faller bort, enten det er ved samtykke fra den som har krav på hemmelighold, ved samtykke fra departementet eller ved kjennelse fra retten, inntrer den alminnelige vitneplikten etter strpl. § 108.[75] Når vitneplikten inntrer for tilbyderen kan også opplysninger som er underlagt taushetsplikt etter strpl. § 204 første ledd, utleveres til politiet.

Tidligere krevde tilbyderne bare et vedtak om oppheving av taushetsplikten for de nærmere angitte opplysninger for å levere de ut. I sin høringsuttalelse til datalagringsdirektivet sa tidligere Post- og Teletilsynet at tilbyderne hadde blitt enige med politiet om at en beslutning om beslag skulle følge begjæringen om å frita tilbyderen fra taushetsplikten.[76] Det vil ikke i stride med reglene at de ber om en beslutning om beslag for noe de kan levere fra seg frivillig, det blir bare en formalisering av en handling de uansett ønsker å bidra til. Som drøftet under kapittel 4.2, kan tilbyder som har fått opphevet taushetsplikten utlevere de aktuelle trafikkdata frivillig til politiet basert på vitneplikten. I motsatt tilfelle må politiet gå veien om et utleveringspålegg.

I brev til Oslo Statsadvokatembeter av 2. mars 2010 gjør Riksadvokaten rede for gjeldende praksis for utlevering av trafikkdata til politiet i forbindelse med etterforskning av straffesaker. Riksadvokaten påpeker at både reglene om beslag i kombinasjon med taushetsfritak og utleveringspålegg etter straffeprosessloven § 210 første ledd kan brukes som hjemler for å innhente trafikkdata, men at det kun er sistnevnte tilfelle som gir en plikt til utlevering. Det står i brevet at "så lenge teletilbyderne godtar at fritak fra taushetsplikt og beslutning om beslag gir tilstrekkelig grunnlag for å medvirke til utlevering av historiske trafikkdata, er det

[74] Andenæs & Myhrer (2009) s. 217 og 221.
[75] Se blant annet Bjerke et.al. (2011) s. 453 og Andenæs & Myhrer (2009) s. 217.
[76] Prop. 49L. (2010-2011) s. 95.

unødvendig å pålegge politiet å gå veien om straffeprosessloven § 210".[77] I forarbeidene til gjennomføring av datalagringskonvensjonen redegjør departementet på samme vis for at både beslag og utleveringspålegg kan brukes som hjemmel til å innhente trafikkdata uten å at forskjellen på hjemlene tas opp til drøfting.[78]

Det er ingen tvil om at ved å bruke reglene om beslag etter strpl. § 203 jf. § 205 i stedet for utleveringspålegg spares både politiet og retten for mye ressursbruk på saksbehandling av saker om utlevering av trafikkdata. Basert på høringsuttalelsen til tidligere Post- og Teletilsynet i forbindelse med innføring av datalagringsdirektivet ville en endring i reglene om bruk av beslag i stedet for utleveringspålegg til å innhente trafikkdata allerede i 2010 medført at tingretten måtte behandlet rundt 2 000 saker årlig om utleveringspålegg. Det er rimelig å anta at dette ville blitt en flaskehals i straffesaksbehandlingen og det er ikke usannsynlig at bruken av sikringspålegg etter straffeprosessloven § 215a første ledd ville økt.

Både beslag og utleveringspålegg betinger at taushetsplikten er opphevet for de aktuelle trafikkdata. Som nevnt over kan en tilbyder som har fått opphevet taushetsplikten be retten prøve gyldigheten av vedtaket. Det vil av den grunn virke overflødig at den samme tilbyderen da skulle be politiet om å gå veien om et utleveringspålegg fordi den ønsket å en rettslig prøving av grunnlaget for beslaget. Der tilbyderen har avstått fra å be retten vurdere gyldigheten av at taushetsplikten oppheves, skulle det være overflødig å be retten vurdere gyldigheten av at politiet ønsker de samme opplysningene utlevert. Tilbyderens motforestillinger mot å utlevere opplysningene må rimeligvis bunne i en uenighet om taushetsplikten skal oppheves, ikke i at politiet skal ha tilgang til opplysninger som tilbyderen da, basert på oppheving av taushetsplikten, har vitneplikt om. For besitteren av bompasseringsdata er utleveringspålegg den nærmeste muligheten for en rettslig vurdering av om de kan utlevere opplysningene mens for den som besitter trafikkdata vil spørsmålet uansett først bli vurdert av Nasjonal Kommunikasjonsmyndighet og vedtaket kan deretter bringes for retten. Å be om et utleveringspålegg for trafikkdata vil bli en form for rettslig dobbelprøving av det samme forhold som skulle være unødvendig.

Reglene om beslag og utleveringspålegg gjelder for historiske trafikkdata. Straffeprosessloven § 216b åpner for at politiet også kan sikre seg fremtidige trafikkdata. Det krever imidlertid at noen mistenkes for et straffbart forhold som kan medføre straff av minst 5 års fengsel eller brudd på bestemte straffebud som angitt i § 216b første ledd bokstav b. Denne bestemmelsen faller utenfor tema for oppgaven og er derfor ikke drøftet.

[77] Riksadvokaten (2010).
[78] Prop.49L (2010-2011) s. 93 - 94.

Konklusjonen er at utlevering av trafikkdata krever at taushetsplikten for de data som ønskes utlevert, oppheves etter reglene i strpl. § 118 første eller andre ledd. Den som har fått opphevet taushetsplikten sin kan utlevere de aktuelle trafikkdata med hjemmel i vitneplikten etter strpl. § 108. Tilbyderen har ingen plikt til å utlevere data og ønsker den ikke å gjøre dette frivillig, må veien gå om et utleveringspålegg fra retten.

4.4 Om oppheving av beslag

Bevismidler kan deles i tre grupper, vitneforklaringer (og siktedes forklaring), reelle bevismidler og dokumentbevis.[79] Det som skiller dokumentbevis fra reelle bevismidler er at det er innholdet, og ikke tingen i seg selv, som utgjør beviset. Et dokumentbevis kan være både papirdokumenter og datafiler.[80] Kopi av lagrede data som gir opplysninger om en persons bevegelser eller kommunikasjon vil naturlig falle inn i kategorien dokumentbevis. Det er innholdet i de lagrede dataene, ikke datafilen i seg selv, som har verdi som bevis. Det som særlig kjennetegner databevis, men som også vil være aktuelt med andre dokumentbevis i mange saker, er at det tas kopi av originalen. Politiet har da kopien og den beslaget er rettet mot har originalen.

Det enkelte beslag i saken skal oppheves når det ikke lengre er behov for beslaget og senest når saken er endelig avgjort med mindre det vil være behov for å beholde beslaget med tanke på en mulig gjenåpning av saken jf. strpl. § 213 første og andre ledd. Beslag i for eksempel en mobiltelefon skal oppheves hvis den senere viser seg å ikke ha bevisverdi eller at innholdet på telefonen er sikret og selve telefonen ikke lenger har en selvstendig bevisverdi.

Beslaget oppheves ved at den beslaglagte gjenstand leveres tilbake til den beslaget ble gjort hos og hvis beslaget tilhører en annen, gjerne tyvegods, leveres det ut til rette eier jf. § 214 første og andre ledd. Beslag som er objekt for inndragning leveres ikke tilbake jf. strpl. § 2 nr 2 jf. strl. §§ 67 flg.

Hvordan dette stiller seg med beslaglagte datafiler som inneholder opplysninger som er bevis i saken kommer an på hvordan man ser på beslaget. Reglene om tilbakelevering eller inndragning av beslag vil naturlig dreie seg om de reelle bevismidler, dvs de fysiske gjenstandene og eventuelle originaldokumenter som er tatt i beslag. Det vil som regel ikke ha noen hensikt å skulle tilbakelevere kopier som besitteren uansett har originalen av. Et alternativ, som vil være aktuelt ved sikring av data fra databærere, er at filene slettes når saken er endelig av-

[79] Andenæs & Myhrer (2009) s. 163 - 164.
[80] ibid. s. 164.

gjort.[81] Det som sikres ut av speilfiler[82] fra databærere vil være lagt inn i saken som dokumenter mens selve speilfilen kan slettes. De lagrede data oppgaven omhandler er data som vil slettes hos besitteren innen en gitt tid, slik at de dataene som er beslaglagt i saken vil være eneste kopi. Det er naturlig å se slike kopier av lagrede data som dokumenter i saken og at de arkiveres sammen saken når den ar avgjort. Det har også fornuften ved seg at disse opplysningene arkiveres sammen sakens øvrige dokumenter av den grunn at ved en begjæring om gjenåpning av saken vil det ikke være mulig å hente inn dataene på nytt. Opplysningene vil da være slettet hos den opprinnelige besitteren.

[81] se Rt 2011 s. 1188

[82] En speilfil er en nøykatig kopi av det originale lagringsmediet der hele dataområdet kopieres, enten det er i bruk eller ikke. Speilfilen kan da gjennomgås for å finne data som kan brukes som bevis.

5 Oppsummering og konklusjon

5.1 Oppsummering av reglene

Problemstillingen oppgaven har tatt for seg er om opptak av kameraovervåkning, bompasseringsdata, data om betalingstransaksjoner og trafikkdata kan utleveres frivillig av besitteren. Innhenting av elektroniske spor som lagres hos en annen en den opplysningene gjelder berører flere regelsett og det er ulike hjemler for ulike elektronisk lagrede data. Jeg vil oppsummere mine betraktninger når det gjelder likhetene og forskjellene. Den mest fremtredende problemstillingen er om politiet får samtykke til utlevering fra den opplysningene er registrert om. Det er i de tilfeller samtykke ikke gis, eller den som besitter dataene ikke vil samarbeide, de straffeprosessuelle regler må tas i bruk.

5.1.1 Utlevering basert på samtykke

De ulike kategoriene av lagrede data oppgaven omhandler er personopplysninger og kan utleveres til politiet hvis den registrerte samtykker etter reglene i personopplysningsloven § 11 første ledd bokstav c. Også trafikkdata som er underlagt lovbestemt taushetsplikt kan utleveres etter samtykke. Det fremkommer i ekomloven § 2-7 femte ledd, siste punktum.

5.1.1.1 Kameraovervåkning

Det er ikke behov for å innhente samtykke til utlevering av opptak fra kameraovervåking da disse kan leveres ut til politiet etter reglene i personopplysningsloven § 39 siste punktum. Det betinger at den som besitter dataene ønsker å levere ut opptakene. I motsatt fall må veien gå om et utleveringspålegg etter straffeprosessloven § 210 første ledd.

5.1.2 Utlevering der ikke er gitt samtykke

Der den registrerte ikke samtykker til at opplysningene utleveres vil reglene om beslag og utleveringspålegg komme til anvendelse. Her kommer det i betraktning om besitteren en underlagt lovbestemt taushetsplikt eller ikke.

5.1.2.1 Opplysninger som ikke er underlagt lovbestemt taushetsplikt

Bompengeselskap og andre som besitter data om bompasseringer er ikke underlagt lovbestemt taushetsplikt og kan frivillig levere ut dataene til. Hvis de ikke ønsker å samarbeide til å utlevere opplysningen nyttes utleveringspålegg, slik som med opptak fra kameraovervåking som nevnt over. Ved fare ved opphold kan påtalemyndigheten bruke hastekompetansen etter strpl. § 210 andre ledd til pålegge opplysningene utlevert

5.1.2.2 Opplysninger underlagt lovbestemt taushetsplikt

5.1.2.2.1 Betalingstransaksjoner

Betalingstransaksjoner er underlagt lovbestemt taushetsplikt etter finansforetaksloven men den gjelder ikke i for straffesaker. For saker under etterforskning gjelder en lovfestet vitne- og utleveringsplikt for politiet etter straffeprosessloven § 210 tredje ledd jf. § 230 andre ledd.

5.1.2.2.2 Trafikkdata

Trafikkdata er underlagt lovbestemt taushetsplikt som ikke viker for vitneplikten etter strpl. § 108. Nasjonal Kommunikasjonsmyndighet kan ved delegert myndighet oppheve taushetsplikten for nærmere angitte opplysninger og vedtaket kan overprøves av retten. Når taushetsplikten oppheves, inntrer vitneplikten og de samme regler gjelder som om opplysningene ikke var underlagt taushetsplikt.

Hvis den lovpålagte taushetsplikten etter ekomloven § 2-9 første ledd ikke oppheves, kan ikke de aktuelle trafikkdata utleveres til politiet.

5.1.3 Beslag eller utleveringspålegg

5.1.3.1 Beslag

I de tilfellene der den som besitter elektroniske spor har vitneplikt og ønsker å samarbeide med politiet, kan de aktuelle elektroniske sporene utleveres til politiet direkte og tas i beslag etter strpl. § 203.

5.1.3.2 Utleveringspålegg

Hvis den som besitter elektroniske spor ikke ønsker å medvirke til å utlevere bevisene eller ønsker rettens vurdering av gyldigheten av beslaget, må veien gå om et utleveringspålegg fra retten etter strpl. § 210 første ledd som pålegger besitteren å utlevere de nærmere oppgitte data.

5.2 Konklusjon

Reglene for politiets tilgang til opptak fra kameraovervåkning, bompasseringsdata, data fra betalingstransaksjoner og trafikkdata er fragmenterte og ulike i sin art selv om de har det til felles at de er lagret hos tredjeperson. Oppgaven viser at det er behov for å ha kjennskap til reglenes innhold og grenseganger. Formålet var å presentere en oversikt over reglene som gjelder der elektroniske spor er lagret hos en annen enn den dataene gir opplysninger om og viser hvordan de ulike kategoriene elektroniske spor faller inn under ulike deler av regelverket. Det har gitt meg en mulighet for å se et bredt sett av regler i sammenheng samt å se fellestrekk og ulikheter ved politiets tilgang under etterforskningen til de ulike typene elektroniske spor.

Litteraturliste

Litteratur

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

Johansen, M. W., Kaspersen, K., & Skullerud, Å. M. (2001) *Personopplysningsloven Kommentarutgave.* Oslo: Universitetsforlaget

Bjerke, H. K., Keiserud, E. & Sæther, K.E. (2011). *Straffeprosessloven kommentarutgave* (4. Utg.). Oslo: Universitetsforlaget

Andenæs, J., & Myhrer, T. (2009). *Norsk Straffeprosess* (4. Utg). Oslo: Universitetsforlaget

Schartum, D. W. (2000). Lov om behandling av personopplysninger, *Lov og Rett*. 543-566

Engstrøm, B. (2004) Forsikringsselskapers taushetsplikt, *Tidsskrift for* forretningsjus 2004 (nr 3). s. 298-308

Lov og forarbeider

2015	Lov 10 april 2015 nr. 17 om finansforetak og finanskonsern (finansforetaksloven)
2005	Lov 20 mai 2005 nr. 28 om straff (straffeloven 2005)
2000	Lov 14 april 2000 nr. 31 om behandling av personopplysninger (personopplysningsloven)
2005	Lov 8 april 2005 nr. 16 om endringer i straffeloven og straffeprosessloven og om samtykke til ratifikasjon av Europarådets konvensjon 8. november 2001 om bekjempelse av kriminalitet som knytter seg til informasjons- og kommunikasjonsteknologi (lovtiltak mot datakriminalitet).
2004	Lov 25 juni 2004 om endringer i straffeloven, straffeprosessloven og sjøloven mv. (fast promillegrense og avholdspliktregler for større skip, et eget straffebud mot tortur, forklaringsplikt for ansatte i finansinstitusjoner mv.
2004	Forskrift 16 februar 2004 om elektronisk kommunikasjonsnett og elektronisk kommunikasjonstjeneste (ekomforskriften)
2003	Lov 4 juli 2003 nr. 83 om elektronisk kommunikasjon (ekomloven)
1999	Lov 3 desember 1999 nr. 82 om endringer i straffeprosessloven og straffeloven m.v. (etterforskningsmetoder m.v.).
1999	Lov 25 juni 1999 nr. 46 om finansavtaler og finansoppdrag (finansavtaleloven)
1999	Lov 21 mai 1999 nr. 30 om styrking av menneskerettighetenes stilling i norsk rett (menneskerettsloven)
1994	Lov 24 juni 1994 nr. 45 om omdanning av forvaltningsbedrifta Televerket til aksjeselskap.
1988	Lov 10 juni 1988 nr. 40 om finansieringsvirksomhet og finansinstitusjoner (finansieringsvirksomhetsloven) (opphevet)

1985 Forskrift 28 juni 1985 nr. 28 om ordningen av påtalemyndigheten (Påtaleinstruksen)
1981 Lov 22 mai 1981 nr. 25 om rettergangsmåten i straffesaker (straffeprosessloven)
1961 Lov 24 mai 1961 nr. 1 om sparebanker (sparebankloven) (opphevet)
1961 Lov 24 mai 1961 nr. 2 om forretningsbanker (forretningsbankloven) (opphevet)
1915 Lov 13 august 1915 nr. 5 om domstolene (domstolloven)
1887 Lov 1 juli 1887 nr. 5 om rettegangsmaaden i straffesager (straffeprosessloven av 1887)(opphevet)

EMK Konvensjon om beskyttelse av menneskerettighetene og de grunnleggende friheter. Roma, 4. november1950.

Prop.49L (2010-2011) Endringer i ekomloven og straffeprosessloven mv. (gjennomføring av EUs datalagringsdirektiv i norsk rett)
Ot.prp. nr 40 (2004-2005) Om lov om endringer i straffeloven og straffeprosessloven og om samtykke til ratifikasjon av Europarådets konvensjon 8. november 2001 om bekjempelse av kriminalitet som knytter seg til informasjons- og kommunikasjonsteknologi (lovtiltak mot datakriminalitet).
Ot.prp. nr 59 (2003-2004) Om endringer i straffeloven, straffeprosessloven og sjøloven mv. (fast promillegrense og avholdspliktregler for større skip, et eget straffebud mot tortur, forklaringsplikt for ansatte i finansinstitusjoner mv.).
Ot.prp. nr 58 (2002-2003) Om lov om elektronisk kommunikasjon (ekomloven).
Ot.prp. nr 92 (1998-1999) Om lov om behandling av personopplysninger (personopplysningsloven).
Ot.prp. nr 35 (1978-1979) Om lov om rettergangsmåten i straffesaker (straffesakloven).

NOU 1997:19 (1997) Et bedre personvern – forslag til lov om behandling av personopplysninger.
NOU 2003:27 (2003). Lovtiltak mot datakriminalitet. Oslo: Datakrimutvalget.

Rettspraksis

Rt 1992 s. 904
Rt 1998 s. 1839
Rt 2011 s. 1188
Rt 2012 s. 1645
Rt 2013 s. 143

Forvaltningspraksis

Personvernnemda, *Klage på vedtak om pålegg om konsesjonsplikt for helautomatiske bomstasjoner* (PVN-2005-11), 7 mars 2006.

Personvernnemda, *Klage på Datatilsynets vedtak om at Postens utleie av adresselister ikke kan forankres i personopplysningsloven § 8 bokstav f) - Posten Norge AS* (PVN-2004-3), 6 desember 2004.

Datatilsynet, *Konsesjon til å behandle personopplysninger,* 23 mai 2006.

Internettreferanser og Korrespondanse

NRK, Dataene som snudde verden på hodet (2017), https://nrkbeta.no/2017/02/04/dataene-som-snudde-verden-pa-hodet/ (4. Februar 2017).

Autopass, *Personvern,* (2016) http://www.autopass.no/om-autopass/Personvern.

Fjellinjen *Personvern,* (2015) http://www.fjellinjen.no/Om-AutoPASS-avtale/regler-for-personvern/.

Statens Strålevern, *Basestasjoner,* (2014) http://www.nrpa.no/temaartikler/91126/ basestasjoner (19.11.2014).

Statens Vegvesen, e-post, 10 februar 2017.

Riksadvokaten (2010) Brev til Oslo statsadvokatembeter. *Innhenting av historiske trafikkdata – utleveringspålegg og beslag* (2.3.2010).