Straffeprosessuelle metoder rettet mot elektroniske bevis

Av Inger Marie Sunde[1]

1 Problemstilling

Elektroniske bevis er viktige for forfølgning av kriminalitet. Fremgangsmåtene for å sikre dem innebærer jevnlig inngrep i borgernes rettssfære og retten til privat liv, jf. EMK artikkel 8. De må da ha hjemmel i lov, jf. legalitetsprinsippet i norsk rett og lovkravet i EMK artikkel 8.2.[2] Straffeprosessuelle bestemmelser oppstiller vilkår for bruk av metodene (inngangskriterier), angir hvem som har kompetanse til å tillate bruken, og gir regler om kontroll. I tillegg beskriver de hva metodene går ut på.[3]

Spørsmålet er om lovens metodebeskrivelser er *gode*. Visse utviklingstrekk innebærer nemlig store endringer i de situasjoner som bestemmelsene opprinnelig tok sikte på. Hovedårsakene er digitalisering av informasjon og utvikling av nettverksteknologien, særlig Internett. Mer spesifikt har det skjedd (i) en overgang fra bruk av felles telefonnummer til individuelle brukerkonti; (ii) enorme datamengder akkumuleres fordi mye data produseres og svært lite slettes; (iii) effektiv søketeknologi er tilgjengelig; og (iv) det har skjedd en alminnelig fremvekst av datatjenester i et utall andre sammenhenger enn det som har med telefonsamtale å gjøre.

---

1. Inger Marie Sunde er født i 1962. Cand.jur. UiO 1987. Ll.M. Harvard Law School 1992. Førstestatsadvokat Økokrim 1993–2005. Ph.d. UiO 2010. Førsteamanuensis Politihøgskolen i Oslo fra 2010.
2. Konvensjonen gjelder som norsk lov, jf. menneskerettsloven § 2 (lov nr. 30/1999). Hjemmel i formell lov kan også være nødvendig fordi fremgangsmåtene rammes av straffebudene om datainnbrudd, ulovlig avlytting og dataskadeverk, jf. straffeloven 1902 §§ 145 annet ledd, 145a og 291.
3. Straffeprosessloven (strpl.) er lov nr. 25/1981.

Spørsmålet er om det er behov for tilpasning av metodereglene i lys av utviklingstrekkene.

2 Avgrensning og om det videre opplegget

Artikkelen gjelder metoder som søker å utnytte mistenktes bruk av elektronisk utstyr og tjenester. Den omfatter ikke metoder som gjør bruk av elektronisk utstyr for å sikre bevis av annen art, som skjult fjernsynsovervåking, jf. strpl. § 202a, og romavlytting med tekniske midler, jf. strpl. § 216m. Også avlytting/opptak av elektronisk kommunikasjon i medhold av samtykke holdes utenfor (strpl. § 216l).

Drøftelsene gjelder metodebeskrivelsen. Først behandler jeg ransaking, beslag og kommunikasjonsavlytting (punkt 3). Kommunikasjonsavlytting, jf. strpl. § 216a, er den eldste metoden som spesifikt gjelder elektroniske bevis. Den ble regulert i 1915 for saker om rikets sikkerhet.[4] Som generell metode ble telefonavlytting innført i 1992.[5] Bestemmelsene er senere endret og supplert flere ganger. Kommunikasjonsavlytting må skje skjult fordi formålet ellers ville forspilles. De rettssikkerhetsmessige farer er søkt kontrollert ved detaljerte bestemmelser i strpl. kapittel 16a og i kommunikasjonskontrollforskriften.[6]

Utviklingen har ledet til at elektroniske bevis kan sikres ved ransaking og beslag, jf. strpl. §§ 192 flg. og §§ 203 flg. Også disse metodene kan anvendes skjult, jf. strpl. §§ 200a og 208a.

Utviklingstrekkene har satt skillet mellom metodene under press når de anvendes mot elektroniske kilder. Det gir grunn til spørsmål om hvorvidt lovens grensedragning mellom kommunikasjonsavlytting og ransaking/beslag er hensiktsmessig.

I punkt 4 drøftes elektroniske spor. Slike spor er viktige fordi mobil kommunikasjonsteknologi, GPS, fri tilgang til Internett (uavhengig av hvilken terminal som benyttes) og utviklingen av «the Internet of Things» gjør at stadig flere objekter, aktiviteter og sosiale relasjoner kan identifiseres og

4. Lov 24. juni 1915 nr. 5 om kontroll med post- og telegrafforsendelser og med telefonsamtaler.
5. Endringslov nr. 52/1992.
6. FOR-1995–03–31–281 JD.

kartlegges.[7] Straffeprosessloven regulerer de elektroniske sporene ut fra om de stammer fra *lukkede kilder* eller fra *politiets bruk av eget utstyr* uten at man kan si at kilden er lukket. Elektroniske spor fra åpne internettkilder faller utenom, og spørsmålet er om utnyttelsen virkelig er fri, eller om lovhjemmel er nødvendig.

I tillegg vurderes den straffeprosessuelle avgrensningen av tilbyderkretsen, som gjør reguleringen uklar. Til sist stilles det spørsmål ved formålsbegrensningen i spesialbestemmelsene om elektroniske spor.

I punkt 5 drøftes rettslige dokumentasjonskrav vedrørende sikring av elektroniske bevis. Automatiserte fremgangsmåter gjør det vanskelig å få innsikt i hvordan etterforskingen er utført. Dette er en rettssikkerhetsmessig utfordring for både åpne og skjulte metoder.

3 Forholdet mellom ransaking, beslag og kommunikasjonsavlytting

Flere utviklingstrekk tyder på at de metodiske skiller mellom ransaking og beslag på den ene siden og kommunikasjonsavlytting på den andre er i ferd med å brytes ned ved sikring av elektroniske bevis. Det at metodene synes å innebære samme type inngrep, indikerer dette.

Kommunikasjonsavlytting går ut på «*å avlytte samtaler eller annen kommunikasjon til og fra bestemte telefoner, datamaskiner eller andre anlegg for elektronisk kommunikasjon som den mistenkte besitter eller antas å ville bruke*», jf. strpl. § 216a tredje ledd. Metoden rammer den del av privatlivet som gjelder retten til fortrolig kommunikasjon og til fritt og uforstyrret å utvikle sosiale relasjoner.

Adgangen til å ransake gjelder «*bolig, rom eller oppbevaringssted … for å søke etter bevis eller etter ting som kan beslaglegges*», jf. strpl. § 192. Av strpl. § 203 følger det at «*ting som antas å ha betydning som bevis, kan beslaglegges …*».

---

7. Se f.eks. «*The Internet of Things – An Action Plan for Europe*», COM(2009) 278 final: «*One major next step in this [Internet] development is to progressively evolve from a network of interconnected computers to a network of interconnected objects, from books to cars, from electrical appliances to food, and thus create an 'Internet of things'*»; Rolf Weber, *Internet of Things – Legal Perspectives*. Sveits 2010.

Den gang ransaking og beslag kun rettet seg mot fysiske rom og objekter, var ransaking en fredsforstyrrelse. Beslag av fysiske objekter var i første rekke et inngrep i eiendomsretten. Kommunikasjonskontroll gjaldt et kvalitativt annet område for livsutfoldelse og ble regulert separat.

Ransaking av *elektroniske (virtuelle) rom* og beslag i *data* synes derimot i første rekke nettopp å innebære inngrep i kommunikasjon og uforstyrret utvikling av sosiale relasjoner. De tilsvarer dermed inngrepet ved kommunikasjonsavlytting. Nettverksutviklingen medfører at informasjon er underveis fordi det meste av datautstyr og mobiltelefoner kobles til Internett. Hvorvidt inngrepet gjelder tradisjonell telefoni eller elektroniske meldinger, er neppe vesentlig. Symptomatisk nok har meldinger i stor grad erstattet telefoni. Den rike informasjonsutvekslingen på sms/mms, «chat», kommentarer på sosiale medier mv. er en samtale. Kommunikasjon om private og profesjonelle forhold omfatter tekst, lyd, bilde, distribusjon av lenker, filoverføring, bruk av vedlegg osv.

Fleksible virtuelle tjenester følger ikke lovens skille mellom innhold som er lagret (ransaking og beslag) og innhold som overføres (kommunikasjonsavlytting). En brukers utnyttelse av sine konti i nettskyen skjer med en oppkobling som er kommunikasjon, men som bare gjelder *egne* nettressurser. Avlytting gir ikke den type informasjon som er metodens formål, nemlig kommunikasjon *mellom impliserte* i et kriminelt opplegg.

Videre kan en nettbasert tjeneste («konto») tilrettelegge for samarbeid mellom flere, for eksempel om utvikling av dokumenter, felles kalender- og avtaleverktøy og, for den del, en regulær e-postkonto som brukes av flere til å dele informasjon. Aktiviteten er kommunikasjon selv om det hele foregår på ett sted (i hvert fall ser det slik ut for brukeren) og resulterer i data som lagres. Ransaking og beslag (eller utleveringspålegg) må anvendes for å sikre bevis, selv om det som sikres er kommunikasjon.

Dataransaking og beslag representerer derfor inngrep i borgernes rett til privat liv og korrespondanse slik som kommunikasjonsavlytting. EMD synes å likestille metodene. I en sak fra 2007 (Copland) ble det konstatert at «private life» omfatter innholdet i telefonsamtaler, e-post, trafikkdata for telefoni og logger som viser spor etter internettbruk («surfing»).[8] Inngrepet

8. Copland mot Storbritannia, dom 3.7.2007, punkt 41, jf. punkt 11.

i telefonsamtalene likestilles med inngrepene i den lagrete elektroniske korrespondansen og i loggene for de forskjellige tjenestene.

Utviklingen innebærer at ransaking og beslag i flere henseender bør anses som like inngripende som kommunikasjonsavlytting. På den ene siden medfører overgangen fra felles telefonnummer til individuelle kommunikasjonstjenester at *kommunikasjonsavlytting* er *mindre inngripende* enn før med tanke på konsekvensene for uskyldig tredjepart, som familiemedlemmer. Tidligere var familien henvist til bruk av husets fasttelefon, noe som innebar avlytting dersom kontroll først var satt på. I dag er avlytting av mobiltelefon det vanlige og medfører en risiko bare ved kommunikasjon med dette nummeret. Samtaler med andre går fri fordi man bruker egen mobiltelefon.[9]

På den andre siden synes produksjon og lagring av store datamengder å medføre at *ransaking* bør anses som *mer inngripende* enn før, både for siktede og for tredjeparter som ufrivillig eksponeres i forbindelse med etterforskingen. Et illustrerende tilfelle er Rt. 2011 s. 1188, hvor politiet hadde speilkopiert 16 millioner datafiler. Sterke personvernhensyn i favør av uskyldig tredjepart talte for å begrense innsynet i speilkopien (avsnitt 40).

I en annen sak (RG 2009 s. 233) ble omfanget av det materialet som kunne beslaglegges etter ransaking i en bank begrenset, jf. strpl. § 170a. Politiet hadde sikret datamateriale som var «opptil 13 år gammelt», og det var tale om «minst 370 000 lesbare enheter». Lagmannsretten fant at det var uproporsjonalt å beslaglegge materiale mer enn tre år tilbake i tid.

Dataransaking er således en «kraftig» metode som kan skaffe mye materiale. Automatiske søkeverktøy kan raskt gå gjennom det hele. Men bruk av overskuddsinformasjon er ikke lovregulert for ransaking slik som for kommunikasjonskontroll, jf. strpl. §§ 216g og i. Dagens teknologi gir mulighet for rutinemessige søk om straffbare forhold som ligger utenfor siktelsen, for eksempel etter overgrepsbilder, jf. straffeloven 1902 § 204a. Regulering av adgangen til å arbeide på denne måten synes å være et aktuelt lovgivningsspørsmål.

---

9. Per 2012 er det flere sim-kort enn personer i verden. I Vesten er det vanlig med flere sim-kort per person. Kilde: *The Ericsson Mobility Report November 2012* http://www.ericsson.com/ericsson-mobility-report. Fenomenet er velkjent innen politiet fordi stadig skifte av sim-kort vanskeliggjør identifikasjon av mobiltelefon som ønskes avlyttet.

Ytterligere gir rettspraksis signal om at definerende trekk ved metodene er i ferd med å jevnes ut. Utgangspunktet er at ransaking gjelder bevis som *eksisterer på tilslagstidspunktet*, mens kommunikasjonsavlytting gjelder *fremover i tid*. Kommunikasjonsavlytting må *pågå for en periode*, mens ransaking er *en kortvarig aksjon* som avsluttes når ransakingsobjektet er gjennomsøkt. Beslag er nært knyttet til ransaking og retter seg da mot ting man finner under en slik aksjon.

Men i forbindelse med data har rettspraksis lagt til grunn at *ransaking kan pågå over en lengre periode*. Beslutningen om beslag skytes ut til man har avdekket relevant informasjon eller ny informasjon har oppstått. En årsak er at datamengdene er så store at beslutningen om beslag må skje et stykke ut i tid. En annen grunn er at nettbaserte tjenester kan brukes etter at politiet har slått til, slik at nye elektroniske bevis kan oppstå og sikres.

I to avgjørelser fra 2011 (Rt. 2011 s. 296 og s. 1188) så Høyesterett på ransakings- og beslagsbestemmelsene anvendt på *data som forelå på tilslagstidspunktet*. Politiet hadde speilkopiert data uten å skaffe seg innsyn i kopiene. I Rt. 2011 s. 296 skyldtes det et rettslig beslagsforbud, jf. strpl. § 204 (betroelser), mens i Rt. 2011 s. 1188 skyldtes det at speilkopien var så stor at det ikke var hensiktsmessig å se gjennom materialet.

Den førstnevnte saken gjaldt siktedes krav om overprøving av beslag, jf. strpl. § 208. Høyesterett fant ikke at speilkopieringen utløste noen rett til å kreve dette. Kopien skulle først gjennomgås av tingretten, jf. strpl. § 205 tredje ledd analogisk, slik at det beslagsfrie materialet kunne fjernes. De dokumenter som ikke var undergitt taushetsplikt, måtte «*på vanlig måte tilbakeleveres påtalemyndigheten for vurdering og beslutning etter § 205 første ledd*» (39). Bestemmelsen gjelder påtalemyndighetens beslutning *om* å foreta beslag. Forut for beslutningen foreligger ikke beslag, og da gjaldt heller ikke overprøvingsretten.

Følgelig er ikke speilkopien automatisk å anse som en beslaglagt ting, jf. strpl. § 203. Speilkopiering er en faktisk handling hvis rettslige status må vurderes nærmere i forhold til de straffeprosessuelle bestemmelsene. I dette tilfellet var det mest nærliggende å anse kopieringen og den påfølgende håndteringen som ledd i en pågående ransaking. Høyesterett uttalte med henvisning til juridisk teori at

> «rettens gjennomgang [etter § 205 tredje ledd] [er] i realiteten et ledd i en pågående ransaking. Det er først etter denne innledende utsortering, at den virkelige ransaking for å søke etter bevis kan komme i gang. På bakgrunn av denne treffer påtalemyndigheten beslutningen om beslag, en beslutning som så kan kreves prøvet av tingretten etter § 208» (40).[10]

Tilsvarende syn ble lagt til grunn i Rt. 2011 s. 1188. Politiet hadde utført automatiske søk i kopien på 16 millioner filer for å finne frem til data som var relevante for saken. De utplukkede filene var lagt inn i saksdokumentene og sendt forsvarerne til de tiltalte A og C, jf. strpl. § 264. De krevde innsyn i speilfilen, noe politiet motsatte seg. Speilkopieringen var foretatt hos A, som følgelig hadde kildedataene og lite behov for en kopi. I forhold til C, som ikke hadde kildedataene, kom Høyesterett etter en bred drøftelse frem til at bare de dokumenter som var «hentet ut» som følge av søket, var omfattet av «sakens dokumenter». Krav om innsyn utover dette ble derfor avslått også for C. Høyesterett tilføyde at «*dersom politiet skulle hente ut nye dokumenter fra speilkopien, vil tiltalte ha krav på innsyn i disse. Hvilken fremgangsmåte politiet da må benytte, går jeg ikke inn på her – utover å peke på at uthentingen må skje eller reglene om beslag*» (45).

Uttalelsen føyer seg til den linjen man la seg på i den første saken, nemlig at beslag skjer når påtalemyndigheten har tatt stilling til relevansen av det enkelte dokument, jf. strpl. § 205, jf. § 203.[11] Så lenge innholdet er ukjent for politiet, vedvarer ransakingen.

De nevnte tilfeller gjaldt datamateriale som forelå på sikringstidspunktet. En beslektet problemstilling gjelder adgangen til å sikre *bevis som skapes senere på en datakilde under politiets kontroll*. Spørsmålet er praktisk for tjenester som brukes etter at politiet har ransaket og tatt beslag.

En relevant sak er Rt. 2000 s. 1345, som gjaldt innringninger til en beslaglagt mobiltelefon hvor etterforskeren hadde gått inn i samtalene uten å opplyse om sin identitet. Spørsmålet gjaldt om samtalene skulle avskjæres

10. Det ble vist til Hans-Petter Jahre, *Ransaking og beslag hos advokater og revisorer i økonomiske straffesaker*, *Festskrift til Anders Bratholm*. Oslo 1990, s. 251; Knut Svalheim, *Advokaters taushetsplikt*. Oslo 1996, s. 221.
11. Dette innskrenker ikke adgangen til «kollektiv betegnelse» av beslaget, jf. Rt. 1981 s. 1199; 1992 s. 898 og 1995 s. 1831.

som ulovlig ervervet bevis. Høyesterett kom til at beviset kunne føres, og tok utgangspunkt i at politiet «*ikke kunne ha plikt til å slå av den beslaglagte mobiltelefonen*» (s. 1348).

Dette utgangspunktet ble ikke problematisert. Generelt innebærer det at politiet kan være passiv deltaker på en kommunikasjonstjeneste som har vært gjenstand for ransaking og beslag. Politiet har således neppe plikt til for eksempel å logge seg av en Facebook-konto etter å ha fått tilgang. Avgjørelsen åpner imidlertid ikke for rutinemessig å innlede en samtale, fordi det «tilfeldige preg» etterforskerens handling hadde, ble understreket (s. 1348).

Høyesterett gikk lenger og konstaterte at politiet også måtte «*ha adgang til å lese tekstmeldinger eller høre mobilsvarmeldinger som kom inn til mobiltelefonen*» (s. 1348). Synspunktet er på linje med Rt. 1997 s. 470 som gjaldt utlevering av fremtidige trafikkdata, jf. strpl. § 210. Bestemmelsen gjelder «ting» vitnet besitter (sml. «ting» som kan tas i beslag, jf. strpl. § 203). Høyesterett fant at utleveringspålegg kunne gis fremover i tid fordi det avgjørende var om trafikkdataene hadde materialisert seg på utleveringstidspunktet. Senere er fremtidig utlevering av trafikkdata blitt spesialregulert i strpl. § 216b annet ledd bokstav d, og det er gitt en generell bestemmelse om fremtidig utleveringspålegg i strpl. § 210b. Men dette berører ikke det prinsipielle, nemlig at utlevering (og dermed beslag) kan tas i fremtidige «ting», herunder elektronisk innhold.[12] Eventuelle begrensninger krever særskilt hjemmel, og slik begrensning er ikke innført for beslag.[13]

Et motstående hensyn er at grensen mot vedvarende overvåking kan bli vanskelig å trekke. Høyesteretts syn er imidlertid mest realistisk på grunn av den tekniske utjevningen mellom lagrete data og kommunikasjon.

Spørsmålene er svært relevante for sosiale medier. De tilrettelegger for kommunikasjon på ett nettsted, for eksempel på en Facebook-profil, og faller dermed mellom flere metoder. Ransaking og beslag passer ikke så godt fordi innholdet er kommunikasjon. På den annen side kan ikke kommunikasjonsavlytting anvendes fordi metoden gjelder overføring på linjen

12. Det er ikke tvilsomt at «ting» i strpl. §§ 203 og 210 omfatter data, se Rt. 2011 s. 296 (24). Det gjelder også det straffeprosessuelle begrepet «sakens dokumenter», se bl.a. Rt. 2006 s. 1193 og Rt. 2011 s. 1188 (33).

13. Bestemmelsene om «*beslag og utlevering av ting … er av generell karakter … Begrensninger … utover det som er fastsatt i straffeprosessloven, krever særskilt hjemmel*» (Rt. 1992 s. 904, s. 906).

mellom forskjellige kommunikasjonsanlegg og ikke aktiviteten på ett sted i nettverket.[14] Her finnes et vakuum som dataavlesing kunne dekke (overvåking av en brukerkonto eller en datamaskin). Det ville skape en sammenheng mellom kommunikasjonskontroll og dataransaking som etter dagens forhold bør anses godt begrunnet.[15]

Imidlertid oppstår usikkerhet fordi metodebestemmelsene ikke er tilpasset det virtuelle rom og rekkevidden av Høyesteretts føringer kan være vanskelig å fastslå konkret. Samtidig gir den alminnelige bruk av nettbaserte tjenester stadig mulighet for å sikre slike bevis.

Til sist ligger den *praktiske utnyttelsen* av kommunikasjonsavlytting ofte nær ransaking og beslag. Med hjemmel i strpl. § 216a kan det gjøres opptak av kommunikasjon, slik at avlyttingen skjer i ettertid. Kommunikasjonen er lagret elektronisk innhold som må gjennomgås for å finne bevis. Den etterfølgende håndteringen er en «analyse» lik den som foretas når data er sikret ved ransaking. Konseptuelt er det neppe noe til hinder for at utvelgelsen av de relevante deler av kommunikasjonen kunne anses som beslag i elektronisk innhold.

Mye tyder på at metodene *kunne reguleres under ett*. En felles metodebestemmelse burde løftes ut av reglene om ransaking og beslag av fysiske rom og objekter. Det vil også være noen spørsmål knyttet til behandling av elektronisk arkivmateriale, regnskaper mv. som jeg ikke har gått inn på her.

Rettsteknisk og pedagogisk ville en felles metodebestemmelse representere en betydelig forenkling og bidra til å oppstille klarere og mer forståelige grenser for metodene. For individet er det mer vesentlig om metoden er skjult, hva som gjelder for håndtering av overskuddsinformasjon, og om det hersker gode kriterier og ordninger for kontroll.

4 Elektroniske spor

«Elektroniske spor» er ikke rettslig definert, men en vanlig forståelse er at det er spor etter bruk av elektronisk utstyr og tjenester. De har flere spesi-

14. Bjerke, Keiserud, *Straffeprosessloven kommentarutgave*. Pkt. 4 til strpl. § 216a.
15. NOU 2009: 15 *Skjult informasjon – Åpen kontroll* (Metodekontrollutvalget) er negativ til dataavlesing som etterforskingsmetode, men foreslår det som gjennomføringsmåte for hemmelig ransaking og kommunikasjonsavlytting. Kapittel 23. Utredningen er til behandling i departementet.

albetegnelser, for eksempel «lokaliserings-, trafikk- og identifikasjonsdata». I en viss utstrekning omfattes også ytringer og annet digitalt innhold, nemlig når det er tilgjengelig fra åpne kilder på Internett. Slike spor sier ikke bare noe om hvor man har vært, men også om hva man har gjort. Sporene er selvsagt også å anse som elektroniske bevis.

Elektroniske spor kan være lagret, for eksempel logger på en datamaskin som viser oppkoblinger til Internett, transaksjonsdata med internettlogger i en nettbank eller en logg over passeringer av elektronisk bomring. Videre kan elektroniske spor sikres i sann tid, for eksempel lokaliseringsdata fra mobiltelefon (basestasjonsdata) som politiet følger idet de genereres. I sum utgjør altså «elektroniske spor» en broket gruppe opplysninger.

Metodebestemmelsene regulerer tilgang til elektroniske spor fra *lukkede kilder*, jf. strpl. § 216b annet ledd bokstav d (kommunikasjonskontroll) som bestemmer at

> «eier eller tilbyder av nett eller tjeneste som benyttes ved kommunikasjonen, skal gi politiet opplysninger om hvilke kommunikasjonsanlegg som i et bestemt tidsrom skal settes eller har vært satt i forbindelse med [mistenktes kommunikasjonsanlegg], og andre data knyttet til kommunikasjon».

Utenfor dette området er de generelle bestemmelsene om ransaking, beslag og utleveringspålegg anvendelige.

Videre reguleres situasjonen når tilgang oppnås ved *bruk av politiets tekniske utstyr* uten at kilden kan anses lukket. Kilden sender signaler som kan fanges opp med peileutstyr. Strpl. § 216b annet ledd bokstav c (kommunikasjonskontroll) gir adgang til «*å identifisere [mistenktes kommunikasjonsanlegg] ved hjelp av teknisk utstyr*», og strpl. § 202b (teknisk sporing) til at «*teknisk peileutstyr [kan] plasseres på kjøretøy, gods eller andre gjenstander for å klarlegge hvor den mistenkte … befinner seg*». Peileutstyr kan også plasseres i klær og gjenstander mv. som den mistenkte bærer på seg eller med seg (§ 202c).

I dag forventes politiet også å utnytte elektroniske spor fra «åpne kilder» på Internett. Dette er ikke metoderettslig regulert.

Første spørsmål er om legalitetsprinsippet tilsier at lovhjemmel er nødvendig for å utnytte elektroniske spor fra slike åpne kilder. Spørsmålet stilles

fordi retten til privat liv også gjelder i det offentlige rom, selv om det kan være usikkert nøyaktig hvilke aspekter som da vernes.

Et generelt utgangspunkt for den rettslige vurderingen finnes i en sak om EMK artikkel 8 fra 2001 (P.G. og J.H.) som gjaldt hemmelig lydopptak foretatt på offentlig område (en politistasjon og en varetektscelle).[16] EMD konstaterte at privat liv «*is a broad term not susceptible to exhaustive definition*». Forskjellige aspekter av privat liv ble gjennomgått, herunder at privat liv også omfatter uforstyrret sosialt samkvem «*even in a public context*» *(56)*.

Spørsmålet var så om lydopptaket representerte brudd på en berettiget forventning om å kunne prate fritt uten å måtte ta en slik risiko i betraktning. EMD kom til at *individets* rimelige forventning om privat liv var «*a significant, although not conclusive factor*» *(57)*. Det er dermed tale om en rettslig standard («berettiget forventning om privat liv») som må vurderes i lys av objektive og subjektive momenter. Saken viser også at kategoriske slutninger ikke kan trekkes av skillet mellom offentlig og privat område. Overført til nettet innebærer det at privat liv kan være utsatt for inngrep selv om opplysningen stammer fra en såkalt «åpen kilde». Hvorvidt det er tilfelle, må vurderes konkret.

Internett som plattform for sosiale aktiviteter og lagringsplass for brukergenerert innhold medfører at politiet har mindre behov for å lagre data lokalt, fordi man kan regne med at dataene er direkte tilgjengelige på nettet. Opplysninger som først er spredt, slettes ikke, de akkumuleres og er søkbare. «Big data» er en formidabel ressurs, men har også utløst en internasjonal debatt om hvorvidt personvernet omfatter en «rett til å bli glemt», som gjelder tiltak for å slette persondata og for å redusere søkbarheten av personnavn. Fremtidens «informasjonsvinner» er den som mest effektivt kan utnytte tilgjengelige data. For politiet representerer det en ny tilnærming i metodebruken.

Det betyr at rettslige normer utviklet med tanke på *etterfølgende* behandling av personopplysninger, ikke gir særlig veiledning, fordi problemet gjelder kartleggingen direkte på kildene.[17]

16. P.G. og J.H. mot Storbritannia, dom 25.9.2001.
17. Saker som Rotaru mot Romania (dom 4.5.2000) og Segerstedt-Wiberg mot Sverige (dom 6.6.2006) er derfor ikke direkte relevante.

Noen momenter av objektiv art er at det for det første bør avklares hva som menes med «åpne kilder». Videre synes graden av intensitet mot en bestemt person å ha betydning, og i tillegg hvorvidt utnyttelsen omfatter opplysninger som ikke var ment for offentligheten, men som likevel var tilgjengelige.

På den subjektive siden synes det relevant om individet kan overskue kartleggingsmulighetene. Til sist har man hensynet til individets mulighet for å skjerme sine opplysninger. Det har både en objektiv og en subjektiv side, fordi det innebærer spørsmål om hvorvidt mulighet for skjerming faktisk tilbys, og om individet har kunnskap og ferdigheter til å utnytte den.

Uttrykket «åpne kilder» tyder på at kildene og/eller opplysningene er enkelt tilgjengelige for alle og enhver. Dette må avgjøres konkret. Men noen tjenester lar seg ikke kategorisere ut fra den binære tilnærmingen åpen/lukket. For eksempel betegnes sosiale medier som «halvoffentlige». Kilden er ikke «åpen» fordi profilen (brukerkontoen) er privat, og er ikke «lukket» fordi innholdet gjerne får vid spredning.

Det er også spørsmål om hvorvidt brukeren frivillig eksponerer sine data. Graden av frivillighet bør vurderes i lys av hvilke muligheter brukeren har til å skjerme dataene. En mulighet er å justere «privacy»-innstillingene, men det avhenger av innsikt og ferdigheter. Tjenesteyterne foretar ofte endringer som påvirker den private statusen, så brukere som ikke følger med kan ufrivillig legge igjen elektroniske spor. Dette bør anses som et tungtveiende hensyn fordi Internett og sosiale medier er så viktige at en stor del av befolkningen ikke kan la være å delta. Til sammenligning har mangelen på valgfrihet begrunnet streng regulering av telefonavlytting.

Dessuten tilsier omfanget av elektroniske spor at kunnskapen som kan skaffes er langt større enn individet har mulighet til å forestille seg. Ideen om at utstrakt informasjonsdeling er et gode, gjelder langt mer enn *ytringene*. I stor grad deles opplysninger om hvor man er og hvor man har vært over et tidsrom, fordi GPS-teknologi er integrert i sosiale medier. Bruk av mobil trådløs oppkobling medfører at brukernes bevegelser kan følges over nett. Gode kartverk visualiserer posisjonen. Sporene kan kobles til hva man har sagt og gjort på sosiale medier og andre nettsteder. Markedet for tjenester som kan utnytte elektroniske

spor tilbyr teknisk utstyr, ferdigheter og analytisk kompetanse. Det gir mulighet til å avdekke identitet bak anonyme innlegg og hvem som inngår i sosiale nettverk. Profesjonell utnyttelse kan derfor berøre privat liv i en vesentlig større grad enn individet aner, og utfordrer legitimiteten av uttrykket «åpne kilder».

Man kan altså forholdsvis enkelt finne momenter som tilsier at lovhjemmel er nødvendig. Men til sist avhenger vurderingen av både kunnskap om hvilke forventninger befolkningen faktisk har, og hvilke fremgangsmåter som tenkes brukt.

Neste spørsmål gjelder straffeprosesslovens regulering av elektroniske spor *når kilden er lukket* og sporene må utleveres fra tilbyder, jf. strpl. § 216b annet ledd bokstav d. Forholdet er at bestemmelsene om kommunikasjonskontroll begrenser seg til «*eier eller tilbyder av nett eller tjeneste som benyttes ved samtalen eller kommunikasjonen*», jf. strpl. § 216a siste ledd. Disse kan pålegges å utlevere trafikkdata og andre data (som lokaliseringsdata) knyttet til elektronisk kommunikasjon.

Uttrykket i strpl. § 216a er koblet til definisjonen i ekomloven § 1-5 nr. 14 som omfatter tilbydere av «*tilgang til nett eller tjeneste*».[18] Det er tilbydere av fasttelefon, mobiltelfon og internettilgang. Tjenester som vi kjenner som «apper» og sosiale medier, omfattes ikke av ekomlovens regulering selv om de rent funksjonelt er tjenester for kommunikasjon. Det gjelder tilbydere av populære tjenester som Skype, Gmail og Facebook, og av spill som World of Warcraft og FIFA (spill som integrerer sanntidstale (IP-telefoni)).

Spørsmålet er om slike tilbydere likevel omfattes av straffeprosessloven. Siste ledd i strpl. § 216a siste ledd tyder på det, fordi kommunikasjonskontroll kan utføres «*uten hensyn til hvem som eier eller tilbyr nett eller tjeneste*». Men formålet er å gjøre det klart at kommunikasjonskontroll kan utføres uten hensyn til om kommunikasjonsnettet er åpent eller lukket, offentlig eller privat.[19] Sondringene svarer ikke på om man har med en kommunikasjonstjeneste som sådan å gjøre. Hvis fortolkningen ikke skal

18. Ekomloven er lov nr. 83/2003. Ekomloven ga også bestemmelser om endringer i strpl. §§ 118, 211 og 216a som dermed tok inn ekomlovens begrepsbruk.
19. Bjerke, Keiserud, *Straffeprosessloven kommentarutgave*. Pkt. 8 til strpl. § 216a.

legge ekomlovens begrepsbruk til grunn, kan man spørre hvor heldig det var å implementere begrepsbruken i straffeprosessloven.

Ved implementeringen av datalagringsdirektivet i 2011 presiserte lovgiver at tilbydere som falt utenom ekomloven, ikke var omfattet.[20] Når bestemmelsene i lov om datalagring trer i kraft, markeres et skille mellom tilbydere som omfattes av straffeprosessuell særregulering for elektroniske spor, og andre tilbydere. Det gir ulik grad av rettslig vern til tross for at inngrepene i individets rettssfære er like. Det er uheldig, for eksempel er det neppe mindre inngripende for privatlivet om utlevering skjer fra Facebook, enn om det skjer fra NetCom.

Ytterligere et problem er at det rent faktisk kan være vanskelig å si *hvem* som yter en bestemt tjeneste, og å vite om vedkommende er å henregne til tilbyderkretsen i strpl. § 216b annet ledd bokstav d. Ta for eksempel «silent sms» som gir sanntidsinformasjon om den geografiske posisjonen til en mobiltelefon. Lojal bruk av bestemmelsen fordrer at det tas stilling til om tjenesten ytes av mobiltilbyder eller av en annen type tjenesteyter. Det er vanskelig å se at problemstillingen i det hele tatt burde være metoderettslig relevant.

Den tredje og siste problemstillingen gjelder politiets *bruk av eget utstyr* for å sanke elektroniske spor. I disse tilfellene er loven svært spesifikk med hensyn til hva sporene kan brukes til. Ifølge strpl. § 216b annet ledd bokstav c kan de brukes for å identifisere mistenktes kommunikasjonsanlegg. For teknisk sporing kan de brukes for å klarlegge hvor mistenkte befinner seg, jf. strpl. §§ 202b og c. (Teknisk sporing omfatter også gjenstander som sådan, dvs. en annen type inngrep enn mot person.)

Den strenge formålsbegrensningen synes ikke å bidra til å gjøre regelverket mer forutsigbart og fremstår dermed som noe svakt begrunnet. Det illustreres av Rt. 2009 s. 394, hvor identifikasjon var foretatt av mobiltelefon for å avdekke mistenktes identitet. Telefonen var ikke var registrert på mistenkte, men man antok at mistenkte benyttet den. Dette lå utenfor bestemmelsens virkeområde.

---

20. På EU-nivå er det innført regler om pliktig lagring av elektroniske spor som genereres av elektronisk kommunikasjon, jf. direktiv 2006/24/EF (datalagring). Direktivet ble gjennomført i norsk rett ved lov nr. 11/ 2011. Loven er foreløpig ikke trådt i kraft. Avgrensningen av tilbyderkretsen er behandlet i Prop. 49 L (2010–2011) pkt. 7.4. og 8.4.

Mot en så spesifikk lovgivningsteknikk kan det innvendes at det generelt er påregnelig at elektroniske spor fra mobile trådløse kommunikasjonstjenester kan belyse *mange* tema. Det er vanskelig å forstå at elektroniske spor skal stå i en særstilling. Ethvert etterforskingsskritt har et begrenset formål, nemlig å avdekke *bakenforliggende* fakta av større betydning for etterforskingen. Helt åpenbart er det tilfellet for «elektroniske spor» som per definisjon peker på bakenforliggende fakta. Det er neppe sterkere behov for å formålsregulere elektroniske spor enn andre elektroniske bevis. Også data som skaffes ved ransaking og beslag sier noe *om* det forholdet etterforskingen gjelder. De ligger på metaplanet som et *middel til sakens opplysning*, slik som elektroniske spor. Det er nokså utenkelig at loven skulle spesifisere hvilket steg i etterforskingen data skaffet ved ransaking og beslag skulle kunne bidra til å opplyse, det til tross for at også slike data kan inneholde elektroniske spor.

Spørsmålet er om lovgiver er i ferd med å gå seg vill i bestrebelser på å gi tilstrekkelig spesifikke bestemmelser. Resultatet synes ikke å bli mer, men *mindre* forutsigbarhet for enkeltindividet, som ikke spør seg om rekkevidden av den enkelte bestemmelse, men om hva regelverket som helhet tillater av inngrep i privatsfæren. Man skulle anta at legalitetsprinsippet ivaretas ved å bestemme at politiet kan peile teknisk utstyr som mistenkte bruker, og utstyr som politiet har utplassert hos mistenkte. Det gir tilstrekkelig forutsigbarhet om hva inngrepet går ut på, samtidig som det er fleksibelt nok til å omfatte ny teknologi, for eksempel droner, såfremt funksjonaliteten begrenses til peiling.

Etter EMK artikkel 8.2 ligger kravet til formålsspesifisitet på et mer generelt nivå enn det som er gjennomført i lovens metodebeskrivelser. Det som kreves, er angivelse av den samfunnsinteresse som begrunner inngrepet. I dette tilfellet er det tale om etterforsking, jf. strpl. § 226, noe som omfattes av EMK artikkel 8.2, «forebygge uorden og kriminalitet». Følgelig er formålet legitimt og klart angitt. Videre sikrer lovens inngangskriterier og kravene til nødvendighet og forholdsmessighet at metoder bare brukes når inngrepet anses som legitimt. Begrensninger utover dette legger bindinger på etterforskingen som lovgiver har liten forutsetning for å løse på en god måte, og som neppe bidrar til forutsigbarhet om hvor grensene går.

De problemstillinger som her er reist, synes å tilsi behov for en generell straffeprosessuell nyregulering.

5 Noen spørsmål om kontroll

Dokumentasjon av metodebruken er en forutsetning for å kunne føre kontroll med at lovens rammer overholdes. Prinsippet er at politiet skal ha frihet i valg av fremgangsmåte, men i etterkant kreves dokumentasjon med rapporter som legges i sakens dokumenter.

Et aktuelt problem er at loven er nokså ensidig fokusert på å dokumentere det som er gjort. Metodebruk som utnytter dataprogrammer og elektroniske tjenester etterlater få ytre spor, og regler om tilstedeværelsesrett, opptegning og merking av beslag og kontroll med kommunikasjonsavlytting er ikke tilpasset elektroniske bevis. Domstolen går heller ikke inn i denne typen kontrolltema. Dermed er det vanskelig å kontrollere at etterforskingen skjer innen lovens rammer.

Kontrollgrunnlaget består hovedsakelig av loggdata som etterforskerens dataprogram selv genererer. Opplysningene gjelder typisk tidspunkt for iverksettelse av programmet, hvilken maskin/brukerområde det ble anvendt på, hvilke data som ble gjennomsøkt og tidspunkt for å avslutte programmet. Loggdataene integreres i et skjema for politirapport som underskrives av etterforsker.

Problemet er at opplysningene bare er riktige dersom programmet er riktig innstilt og satt opp til å rapportere alle relevante hendelser. Både tilsiktede og utilsiktede feil kan oppstå. Man kan for eksempel tenke seg at det genereres en logg som «opplyser» at programmet ble slått av tidligere enn det som var tilfelle. Det samme kan skje utilsiktet, for eksempel dersom programmet ikke er justert for endringer i tidssone.

Svakheten er at rapporteringen bygger på interne mekanismer i programmet. Loven burde kreve at opplysningene også verifiseres utenfra og etablere egnede kontrollprosedyrer. Kontrollkravet burde gjelde positivt og negativt, dvs. at dokumentasjonen viser det som faktisk er gjort og gir grunnlag for å kontrollere at *ikke annet eller mer er gjort* enn det som står i rapporten.

Den nevnte saken Rt. 2011 s. 1188 illustrerer at det kan være behov for et negativt dokumentasjonskrav. Høyesterett sa at

> «tiltalte må ha krav på en detaljert redegjørelse for de søk politiet har gjort i speilkopiene – for eksempel om filtyper, stikkord og lagringssted. Han har derved mulighet til å kontrollere at han har fått alle de dokumenter som politiet har hentet ut, og dessuten til å vurdere om søkene er foretatt på tilfredsstillende måte» (44).

Redegjørelsen var en forutsetning for at innsynsretten kunne begrenses til de datafiler som var «hentet ut». Løsningen baserte seg på at politiet ikke hadde mer informasjon enn tiltalte fordi man ikke hadde sett på andre filer enn de som var hentet ut (dommen avsnitt 37 og 45). Hensynene til kontradiksjon og partslikhet var derfor ivaretatt.

Men forutsetningen er bare holdbar dersom rapporten er i overensstemmelse med realiteten. Det er mulig for politiet å se på filer uten «å hente dem ut». Søk i 16 millioner filer kan gi et omfattende resultat hvorav bare noen få filer anses som relevante for saken. For å ivareta rettssikkerhetsgarantiene bør hovedregelen være at redegjørelsen omfatter alle nivåer i analysen, men dette følger ikke klart av den siterte uttalelsen.

Et annet eksempel gjelder om politiet skal kunne plassere et skjult dataprogram («trojaner») på mistenktes datamaskin for å lette hemmelig ransaking og kommunikasjonsavlytting. Et slikt forslag er fremsatt i utredningen «Skjult informasjon – Åpen kontroll» fra 2009.[21] Man må regne med at egenrapporten kommer til å opplyse at bare slike data som det gis adgang til å registrere, er blitt registrert, og at trojaneren deretter ble slettet. Spørsmålet er om det kan verifiseres. Burde dokumentasjon kreves for at programmet ikke ble benyttet for eksempel til å foreta romavlytting, at det ikke var aktivt lenger enn opplyst, og at trojaneren var skjermet slik at andre ikke kunne utnytte den mens det lå aktivt på siktedes maskin? Trojaneren er jo en sårbarhet som åpner for inntrengning fra tredjemann.[22]

21. Se fotnote 14.
22. Dataavlesing. Inger Marie Sunde. *Retfærd* 2012 nr. 1/136, s. 3 flg.

Hvorvidt så omfattende dokumentasjonskrav kan oppfylles, er et annet spørsmål. Hvis det ikke er mulig, bør konsekvensene analyseres og ligge til grunn for åpne vurderinger av om en metode i det hele tatt bør tillates.

Slik det arbeides i dag, kan en etterforsker med gode intensjoner og mye initiativ laste ned et program fra Internett og bruke det i jobbutførelsen. Nøyaktig hva som skjedde, vet man bare ut fra dokumenter i saken. Politiet som etat mangler et organ som har til oppgave å kvalitetssikre de verktøy som benyttes i forhold til grunnleggende rettssikkerhetskrav. Det kan være behov for å bygge opp en ny ressurs i takt med at politiet satser stadig mer på å utnytte elektroniske bevis.

Tidligere leder av EOS-utvalget, Helga Hernes, har fremhevet problemet med å kontrollere teknisk betont metodebruk. Hun konstaterer at «*[m]engden kommunikasjon og det store antall forskjellige teknologier øker den totale kompleksiteten. For [EOS-utvalget] er det derfor i dag umulig å føre 100 prosent kontroll med alt som skjer i slike kompliserte systemer*».[23]

Sitatet står til ettertanke. Det er til sist et demokratisk problem om vi godtar inngripende metoder uten at lovgiver dokumenterer at metoden er kontrollerbar, og sørger for bestemmelser som stiller relevante kontrollkrav.

23. *Overvåking i en rettsstat*. Dag W. Schartum (red.) Helga Hernes, *EOS-utvalgets kontroll av «de hemmelige tjenester», s. 319. Bergen 2010*.