Sitering av artikkelen i APA (6th):
Sunde, I. M. (2012). Dataavlesing som etterforskningsmetode.
Retfærd, *35*(1), 3-35.

Dataavlesing som etterforskingsmetode

Inger Marie Sunde, Førsteamanuensis

Abstract

The paper takes a critical approach to a secret investigation whereby the police put the suspect's computer under surveillance. In particular, the use of a secret computer program (a "Trojan horse") on the suspect's computer gives cause of concern. The method has been proposed in Norway and Sweden and was introduced in Denmark in 2002. The analysis shows that designing proper procedural provisions poses considerable challenges to the lawmaker. The author suggests that rules of data search and seizure should be regulated separately from physical search and seizure, and that rules of computer and communication surveillance should be merged into one legal provision.

In addition, the use of a secret program raises serious concerns as to the rule of law. The program creates a "back door" to the suspect's computer. The question is whether it can be shielded against exploitation over the net from third parties. It is argued that unless the state produces sound documentation made by impartial technical experts that confirms that the police program can be shielded from abuse, the method ought not to be introduced in national legal systems. If it has been introduced absent such documentation, it ought to be suspended. The state is responsible for securing its subject's rights when interfered with by the police. If the state cannot provide a guarantee against third party abuse, the method is not controllable and the rule of law seems to be put in jeopardy.

Keywords

Computer surveillance – keylogging - secret computer program - "Trojan horse" - digital search, seizure and interception - principle of legality - rule of law.

1. Problemstilling

'Dataavlesing' er en skjult etterforskingsmetode hvor politiet ved tekniske midler skaffer seg tilgang til innholdet på en datamaskin. Danmark innførte dataavlesing i den såkalte "Terrorpakke 1" (lov nr. 378 av 6. juni 2002) som fulgte opp FNs resolusjoner etter angrepet på Manhattan i 2001.[1] Etter dansk rett anses dataavlesing som en selvstendig etterforskingsmetode og er regulert i en egen bestemmelse, jf. retsplejeloven § 791 b. Metoden er visstnok også innført i enkelte andre europeiske land, samt i USA og Canada.

Både i Norge og Sverige har dataavlesing blitt foreslått innført. Det svenske forslaget gikk ut på å innføre dataavlesing som selvstendig metode slik som i Danmark. Forslaget har ikke blitt fulgt opp.[2]

[1] Se redegjørelse for metoden i Smith (2011) ss. 454 flg., og kritikk av Toftegaard Nielsen (2010).

[2] Dataavlesing ble foreslått innført i Sverige i 2005 i utredningen "Tillgång til elektronisk kommunikation i brottsutredningar m.m." (SOU 2005: 38). Så vidt forstås er ikke forslaget politisk realitetsbehandlet.

Siden Sverige har høy utredningsaktivitet vedrørende politimetoder må spørsmålet likevel stadig anses å være aktuelt.[3]

I Norge er dataavlesing foreslått av Metodekontrollutvalget i utredningen "Skjult informasjon – Åpen kontroll" (NOU 2009: 15) kapittel 23. I skrivende stund er utredningen til behandling i Justisdepartementet. Til forskjell fra i dansk rett foreslås det at dataavlesing *ikke* bør være en selvstendig metode, men en "fremgangsmåte" eller "gjennomføringsmåte", som kan effektivisere hemmelig ransaking, beslag og kommunikasjonsavlytting. Hovedformålet er "at politiet settes i stand til å sikre informasjon som er kryptert eller på annen måte er gjort utilgjengelig".[4] Utvalget foreslår å tilføye en adgang til "å foreta innbrudd i et datasystem" i bestemmelsene om hemmelig ransaking og kommunikasjonsavlytting og opplyser at "reelt sett" er dette bare en "videreføring av allerede eksisterende hjemler."[5]

Forskjellen mellom Metodekontrollutvalgets tilnærming og den danske løsningen er tankevekkende. I samsvar med politiske føringer har Metodekontrollutvalget forsøkt å innføre metoden med presisjon slik at den imøtekommer behov som ikke kan dekkes av mildere inngrep, og heller ikke går lenger enn behovet tilsier. Spesielt har utvalget presisert at forslaget *ikke* åpner for *gjentatt eller fortløpende* ransaking av datasystem (se sitat i pkt. 2.1.3 nedenfor). Forslaget skiller seg her fra den danske løsningen på et vesentlig punkt.

Den restriktive norske holdningen er lojal i forhold til EMKs vilkår om at en lovhjemmel som gir adgang til inngrep i privatsfæren ikke må gå lenger enn "nødvendig i et demokratisk samfunn", jf. EMK artikkel 8.2. Spørsmålet er om den norske tilnærmingen oppnår formålet, dvs. å imøtekomme etterforskingsbehovet uten å innebære løpende overvåking av datasystemet. Det er også spørsmål om den lovtekniske løsning oppfyller legalitetsprinsippets krav om at hjemmelen må være klar. Artikkelen vurderer det norske forslaget i lys av disse kriteriene. Under en rettspolitisk synsvinkel drøftes det hvorvidt regler om dataransaking helt bør skilles ut av bestemmelsene om fysisk ransaking.

Artikkelen tar også opp rettssikkerhetsspørsmål. Spørsmålene gjør seg gjeldende uavhengig av om dataavlesing hjemles som selvstendig metode eller som del av andre metoder.

Dataavlesing er et relativt nytt og lite kjent tvangsmiddel og artikkelen har som selvstendig formål å belyse hva metoden innebærer.

Om lovbehandlingen i Norge skulle være fullført når artikkelen publiseres, er spørsmålet om valg av lovgivningsteknikk stadig aktuelt for Sverige. Rettssikkerhetsdrøftelsen er dessuten relevant også om metoden er innført, dvs. for *alle* land som har innført dataavlesing, også utenfor Skandinavia.

Drøftelsene konsentrerer seg om prinsipielle spørsmål knyttet til metodens karakter og går ikke inn på en detaljert behandling av inngrepsvilkårene m.v., etter det enkelte lands rett. Formålet er å fokusere på de mer gjennomgripende perspektiver ved metoden.

---

[3] Polismetodutredningen (Ju 2008:01) gjelder politiets skjulte metodebruk og kunne for så vidt ha omfattet dataavlesing. Det er avgitt to delutredninger, en om mer rettssikker innhenting av elektronisk kommunikasjon i etterforskingen (SOU 2009:1), og en sluttbetenkning om skjult metodebruk i politiarbeidet (SOU 2010:103). Betenkningene ser ikke ut til å berøre dataavlesingsspørsmålet.

[4] NOU 2009: 15 s. 237.

[5] NOU 2009: 15 s. 244.

Terminologisk betegner jeg dataavlesing som en "metode" med mindre konteksten er å effektivisere en annen metode. I det siste tilfellet betegner jeg dataavlesing som en "fremgangs-" eller "gjennomføringsmåte" av "primærmetoden", dvs. hemmelig ransaking, beslag og kommunikasjonsavlytting.

2. Beskrivelse av norsk og dansk modell for dataavlesing

2.1 Presentasjon av Metodekontrollutvalgets forslag

2.1.1 Den lovtekniske tilnærmingen

I den *lovtekniske* tilnærmingen tok Metodekontrollutvalget utgangspunkt i at dataavlesing som fremgangsmåte betraktet, burde anses som *datainnbrudd* som kan hjemles ved tilføyelser i staffeprosessloven § 200a om hemmelig ransaking og straffeprosessloven § 216a om kommunikasjonsavlytting.

Tilføyelsene lyder slik:

Hemmelig ransaking: Straffeprosessloven § 200a første ledd nytt siste punktum:

"Retten kan gi politiet tillatelse til samtidig eller senere *å foreta innbrudd i et datasystem* for å kunne gjennomføre ransaking etter bestemmelsen her." (min uth.).

Kommunikasjonsavlytting: Straffeprosessloven § 216a, nytt fjerde ledd:

"Dersom kommunikasjonsavlyttingen er vanskeliggjort på grunn av teknologiske eller andre innretninger, kan retten ved kjennelse gi politiet tillatelse til *å foreta innbrudd i et datasystem* for å kunne gjennomføre kommunikasjonsavlyttingen." (min uth.).

Utvalget mener at datainnbrudd kan effektivisere hemmelig ransaking, databeslag og kommunikasjonsavlytting. Dessuten skal det gi klar hjemmel for ransaking over nett ("on line" ransaking).

Ransaking over nett savner ifølge utvalget "klar rettskildemessig forankring" etter gjeldende rett.[6] På dette punkt innebærer forslaget følgelig er en reell utvidelse av inngrepsadgangen. Utvalget har derfor ikke sine ord helt i behold når det sier at forslaget bare er en "teknologisk tilpassing" som "reelt sett" viderefører allerede eksisterende hjemler.[7]

Utvalget ser ikke behov for tilføyelse i bestemmelsen om hemmelig beslag, jf. straffeprosessloven § 208a, fordi datainnbruddet bare berører *atkomsten* til dataene, ikke beslag etter at atkomst er oppnådd.[8] Beslag kan tas uavhengig av hvordan atkomst er oppnådd.

2.1.2 Datainnbrudd ved kommunikasjonsavlytting

For *kommunikasjonsavlytting* er formålet med lovendringene utdypet på s. 245 i Metodekontrollutvalgets utredning:

Datainnbrudd skal gi politiet mulighet "for å kunne gjennomføre kommunikasjonsavlyttingen, dersom avlyttingen er vanskeliggjort på grunn av teknologiske eller andre innretninger." Hjemmelen gir ikke adgang til å skaffe politiet "full kontroll med systemet". Adgangen begrenses til utelukkende

[6] NOU 2009: 15 s. 246.
[7] NOU 2009: 15 s. 244.
[8] NOU 2009: 15 s. 246, spalte 2 nederst.

å gjelde "opplysninger som relaterer seg til vanskeliggjøringen av kommunikasjonsavlyttingen". Det gis ikke adgang til å skaffe data som er lagret. Da må "bestemmelsene om hemmelig ransaking og beslag anvendes".

Begrunnelsen refererer seg til *krypteringsproblemet*. Endringen skal sikre at politiet får fatt i den kommunikasjon (mellom kommunikasjonsanlegg) som dagens regler alt gir adgang til. Teknologiutviklingen har medført at både de kriminelle selv og profesjonelle tjenesteytere som ledd i leveransen av en sikker tjeneste, bruker kryptering. Det kan medføre at kommunikasjonen er forvansket og verdiløs for etterforskingen. Metodekontrollutvalgets tanke synes å være at ved innbrudd på kommunikasjonsanlegget kan politiet få fatt i kommunikasjonen *før* den krypteres eller *etter* at den er dekryptert. På vei ut/inn av datamaskinen er kommunikasjonen i klartekst ellers kunne ikke mistenkte føre en samtale. Dessuten opplyser utvalget at politiet kan fange opp *kodenøkler* som kan dekryptere kommunikasjonen i transportfasen.[9]

Følgelig gis det adgang til å fange opp *kodenøkkel* som kan dekryptere kommunikasjon i sann tid, men ikke kodenøkkel som kan dekryptere lagrete data på mistenktes datamaskin. Det gis heller ikke adgang til å fange opp *tilgangsdata* for å utføre datainnbrudd ved hemmelig ransaking. Politiet vil altså ikke kunne skaffe seg tilgangsdata til bruk for hemmelig "on line" ransaking ved først å koble opp kommunikasjonsavlytting. Metodebruk mot lagrete data og datasystemet som sådan faller nemlig utenfor kommunikasjonsavlyttingsbestemmelsens saklige virkeområde.

2.1.3 Datainnbrudd og hemmelig ransaking og beslag

Datainnbrudd på datasystem skal også effektivisere hemmelig ransaking og beslag. Metodekontrollutvalget viser her til *to begrunnelser* og det er nødvendig å sammenholde spredt informasjon på ss. 240-246 for å få fatt i dem.

Den ene gjelder *krypteringsproblemet*, dvs. at data lagret på mistenktes datamaskin kan være kryptert og uleselig i forbindelse med beslag. Det opplyses at dataavlesing vil kunne tenkes

"å åpne for avlesing av mistenktes passord, og dermed lettere gi tilgang til den aktuelle informasjonen på maskinen, i programmer eller i dokumenter ved ransaking og beslag" (s. 242).

Hvilke beslagssituasjoner som kan være aktuelle er ikke beskrevet.

Videre opplyser utvalget at adgangen til å foreta datainnbrudd er ment å klargjøre at ransakingsbestemmelsen gir *adgang til å foreta ransaking over nett*, dvs. ransaking uten politiets fysiske tilstedeværelse. Det opplyses at i underrettspraksis har det vært gitt adgang til slik ransaking, men at "det savner en klar rettskildemessig forankring" (s. 246). Utvalget støtter imidlertid fremgangsmåten, på grunn av behovet og fordi det antas regulært å være mindre inngripende enn hemmelig fysisk ransaking.

Forslaget åpner imidlertid *ikke for gjentatt* eller *fortløpende* ransaking. Slik ransaking ville

[9] "Dataavlesing kan tenkes å gi politiet adgang til for eksempel å avlytte kommunikasjonen før den blir kryptert, alternativt skaffe seg krypteringsnøkkelen på mistenktes datamaskin for så å dekryptere meldingen i transportfasen" (NOU 2009: 15 ss. 241-242).

”innebære en klar utvidelse av dagens adgang til bruk av hemmelig ransaking, fordi det vil gi politiet anledning til systematisk å kartlegge mistenktes bruk av et datasystem over tid, herunder opplysninger som ikke blir lagret i datasystemet og dermed ikke vil kunne hentes ut ved tradisjonell hemmelig ransaking. Etter utvalgets syn er dette en for stor integritetskrenkelse i forhold til det anførte behovet” (s. 246).

2.2 Den danske bestemmelsen om dataavlesing

Den *danske bestemmelsen* om dataavlesing i retsplejeloven § 791 b, er en selvstendig metodebestemmelse som står i kapittel 71 sammen med bestemmelser om inngrep i meddelelseshemmeligheten, observasjon og forstyrrelse eller avbrudd av radio- og telekommunikasjon. Jeg siterer retsplejeloven § 791 b første, tredje og fjerde ledd (stk.). Stk. 2, inneholder en påminnelse om at proporsjonalitetsprinsippet gjelder.

”Stk. 1. Avflæsing af ikke offentlig tilgængelige oplysninger i et informationssystem ved hjælp af programmer eller andet utstyr (dataflæsning) kan foretages, såfremt

1. der er bestemte grunde til at antage, at informationssystemet anvendes af en mistænkt i forbindelse med planlagt eller begået kriminalitet som nævnt i nr. 3,
2. indgrebet må antages at være af avgørende betydning for efterforskningen, og
3. efterforskningen angår en lovovertrædelse, som efter loven kan straffes med fængsel i 6 år eller derover, en forsætlig overtrædelse af straffelovens kapitel 12 eller 13 eller en overtrædelse af § 289.

Stk. 3. Afgørelse om dataaflæsning træffes af retten ved kendelse. I kendelsen angives det informationssystem, som indgrebet angår. I øvrig finder reglerne i § 783, stk. 1, 3. og 4. pkt., samt stk. 3 og 4, tilsvarende anvendelse.

Stk. 4. Efterfølgende underretning om et foretaget indgreb sker efter reglerne i § 788, stk. 1, 3 og 4. Underretningen gives til den, der har rådigheden over det informationssystem, der har været aflæst efter stk. 1. I øvrig finder reglerne i § 782, stk. 2, §§ 784, 785, 789 samt 791 tilsvarende anvendelse.”

Smith (2011) redegjør for metoden med henvisning til forarbeidene på ss. 454 flg.. Bakgrunnen for bestemmelsen er at politiet ved etterforsking av alvorlig kriminalitet

”kan have behov for løbende at kunne registrere innholdet og anvendelsen af bestemte computere. Dette kan for eksempel ske gennem installering af ”særlige edb-programmer, såkaldte ››sniffer-programmer‹‹” (s. 455).

Følgelig gir bestemmelsen politiet adgang til å foreta løpende avlesing av aktivitet på datamaskinen. ”Sniffer-programmet” kan for eksempel sørge for at politiet

”automatisk får tilsendt en kopi af alle meddelelser afsendt fra den mistenktes computer, ligesom programmet vil gøre det mulig for politiet løbende at registrere samtlige indtastninger, som brugeren af computeren foretager. Endvidere kan edb-programmer af den omtalte karakter gøre det mulig for politiet automatisk og uden brugerens vidende at modtage kopi af e-post, der afsendes fra eller modtages af en computer, samt af opslag på internettet. De elektroniske meddelelser, som er sendt til mistænkte, og som opbevares i computerens hukommelse, vil ligeledes være omfattet af indgrebet.” (s. 455).[10]

Dataavlesing etter dansk mønster er følgelig en metode *av vedvarende karakter.* Hvorvidt den gir hjemmel for *gjentatt overvåking* innenfor det angitte tidsrom har jeg ikke sett vurdert. Spørsmålet har en side til retsplejeloven § 799 stk. 3, som gir hjemmel for *gjentatt ransaking, men ikke for fortløpende (vedvarende) ransaking*. Dataavlesingsbestemmelsen avgrenser tidsrommet etter tilsvarende regler som for kommunikasjonskontroll (”indgreb i meddelelseshemmeligheden”), noe

[10] Sml. Gomard (2008) note 3. til retsplejeloven § 791b.

som betyr at det kan gis tillatelse til dataavlesing for inntil 4 uker av gangen. Også *begrensningene* for kommunikasjonsavlytting for så vidt gjelder bruk av dataene som bevis m.v., og pålegg om tilintetgjørelse av data, gis anvendelse for dataavlesing. Dette følger av henvisningen til retsplejeleoven §§ 789 og 791 i retsplejeloven § 791 b stk. 4.

Dataavlesingsbestemmelsen i retsplejeloven begrenser ikke *hvilken type data* som kan fanges opp. Den gir således adgang til å fange opp (i) data som skrives til datamaskinen, men ikke lagres, slik som passord og kodenøkler. Det har ikke betydning om kodenøklene gjelder sanntidskommunikasjon, lagrete data eller om det er tale om tilgangskoder til et datasystem; (ii) data som sendes ut/inn av datamaskinen, uavhengig av om dataene også lagres; og (iii) data som er lagret på datamaskinen (historiske data).

2.3 Sammenligning

I det følgende sammenligner jeg det materielle innholdet av den norske og danske løsningen.

2.3.1 Inngrepets varighet

En vesentlig forskjell gjelder inngrepets varighet. Den danske hjemmelen gir adgang til vedvarende overvåking av datasystem for inntil 4 uker av gangen. Det norske forslaget gir bare adgang til datainnbrudd. Når tilgang er oppnådd følger inngrepet reglene for primærmetoden. For kommunikasjonskontroll er hovedregelen en tidsramme på inntil 4 uker av gangen, jf. straffeprosessloven § 216f. For ransaking er regelen at inngrepet er tidsmessig strengt avgrenset. Når ransaking først er innledet må inngrepet avsluttes så snart gjennomsøkingen er gjennomført. Ransaking kan ikke ta form av vedvarende overvåking av ransakingsobjektet. I datasammenheng ville det være det samme som å anvende dataavlesing som selvstendig metode.[11]

2.3.2 Avgrensning av den informasjon som kan fanges opp

Den danske løsningen begrenser ikke hvilke data som kan fanges opp, noe det norske forslaget nettopp tilsikter. Begrensningene kan ikke leses direkte ut av ordlyden i de norske bestemmelsene, men må innfortolkes på bakgrunn av *primærmetodens art*. Sitatet fra Smith (2011) i kapittel 2.2, gir eksempler på hva retsplejeloven § 791 b gir adgang til å fange opp. Eksemplene kan brukes for å sammenligne bestemmelsenes rekkevidde. Jeg sorterer eksemplene i gruppe (i)-(iii) som over.

De *etterfølgende* restriksjonene i dansk rett som gjelder bruk av dataene som bevis og tilintetgjørelse av data, vil etter norsk rett bare gjelde data innhentet ved kommunikasjonsavlytting, jf. strpl. §§ 216g og i. Bestemmelsen om hemmelig ransaking, strpl. § 200a, viser ikke til de nevnte bestemmelsene.

(i) Smith (2011) nevner mulighet for *"løbende at registrere samtlige indtastinger, som brugeren af computeren foretager"*. Dette er *data som skrives til datamaskinen*.

Det norske forslaget er vesentlig mer begrenset fordi det bare gir adgang til å fange opp informasjon som *bidrar til* å gi kommunikasjon i klartekst, til å begå datainnbrudd ved hemmelig ransaking og til å dekryptere beslag. Med andre ord omfattes *kodenøkler og tilgangskoder*. Hvilke koder som kan fanges opp avhenger av hvilken hjemmel som er grunnlag for inngrepet. Løpende bruk av datasystemet kan uansett *ikke* fanges opp.

(ii) Videre gis dansk politi adgang til *"uden brugerens vidende at modtage kopi af e-post, der afsendes fra eller modtages af en computer, samt af opslag på internettet".* Dette er *data*

[11] NOU 2009: 15 s. 246.

som kan fanges opp under overføring på vei ut/inn av datamaskinen, dvs. over nettverksforbindelsen. Slik trafikk omfattes av annet alternativ i straffeprosessloven§ 216a tredje ledd "samtaler eller annen kommunikasjon", og kan følgelig etter det norske forslaget registreres med hjemmel i bestemmelsen om kommunikasjonsavlytting.[12] Verken bestemmelsen om hemmelig ransaking eller hemmelig beslag kan brukes for dette formål.

(iii) Til slutt kan dansk politi *"automatisk få tilsendt en kopi av alle meddelelser afsendt fra den mistenktes computer"* (først i sitatet) og *"de elektroniske meddelelser, som er sendt til mistænkte, og som opbevares i computerens hukommelse"* (sist i sitatet). Eksemplene gjelder – så vidt forstås - *data som er lagret*.

Den danske bestemmelsen gir altså adgang til å kopiere lagrete data. Men av eksemplene synes poenget å være at kopien *automatisk* sendes til politiet idet meldingen behandles av mistenktes datasystem. Automatiseringen gjør det unødvendig for politiet å trenge seg inn i datamaskinen med jevne mellomrom for å kopiere data (gjentatt hemmelig ransaking og beslag). Dataene kan fanges opp *automatisk i sann tid*.

Metodekontrollutvalgets intensjon synes å være at hemmelig beslag skal kunne tas i sammenheng med hemmelig ransaking av datasystem. Men til forskjell fra den danske løsningen kan man ikke gå frem automatisert, fordi det innebærer løpende overvåking av datasystemet. Politiet kan bare kopiere i forbindelse med ransaking. Dersom det er aktuelt å foreta databeslag på et senere tidspunkt også, må ny beslutning om hemmelig ransaking innhentes, for å oppnå den nødvendige atkomst til dataene. Gjentatt ransaking er det ikke hjemmel for i norsk rett, og som nevnt, heller ikke foreslått av Metodekontrollutvalget.

Det kan likevel være noe usikkert hva data *"som er sendt til mistænkte, og som opbevares i computerens hukommelse"* innebærer. Det er mulig man har tenkt på data som er mottatt, men ikke aktivt lagret på harddisk eller epostserver. I så fall er dette flyktige data som slettes når datamaskinen slås av. Hvis dataene er kommet inn til datamaskinen, men ikke lagret, kan de anses som *en selvstendig kategori (iv)*. Dette følger av at eksemplet forutsetter at dataene ikke er fanget opp over nettverksforbindelsen (jf. (ii)), ei heller ved inntasting til maskinen (jf. (i)), men likevel at de på et eller annet vis kan fanges opp.

De betyr at politiet må foreta løpende registrering (avlesing), noe det norske forslaget altså *ikke* åpner for. Metodekontrollutvalget presiserer tydelig at systematisk kartlegging av mistenktes bruk av datamaskinen er utelukket, *"herunder opplysninger som ikke blir lagret i datasystemet og dermed ikke vil kunne hentes ut ved tradisjonell hemmelig ransaking"* (se sitatet sist i kapittel 2.1.3).

[12] Se oppsummeringen av gjeldende rett vedrørende kommunikasjonsavlytting i NOU 2009: 15 s. 176. Det fremgår at avlyttingsadgangen omfatter "all informasjonsutveksling mellom kommunikasjonsanlegg, uavhengig av hvilken form eller hvilket innhold informasjonen måtte ha. Dermed omfattes i tillegg til samtaler, overføringer av tekst (herunder e-post), bilde og film." For egen del kan jeg tilføye at også (skadelig) dataprogram som bare datasystemer kan forstå og behandle, omfattes. Det er ikke noe vilkår at innholdet kan forstås av mennesker fordi kommunikasjonsbegrepet følger en teknisk definisjon. Se artikkelen kapittel 5.

2.3.3 Hjemmelsutforming: Betydning for bevisavskjæring og samspill mellom metoder

I motsetning til i dansk rett blir det etter det norske forslaget av stor betydning med hvilken hjemmel dataene fanges opp. Den løpende aktiviteten *på systemet* kan ikke fanges opp, unntatt kodenøkler. Dette gjelder begge metodene, dvs. både straffeprosessloven § 200a (hemmelig ransaking) og straffeprosessloven § 216a (kommunikasjonsavlytting). Dersom *inntastingen* representerer *kommunikasjon i sann tid*, som "chat" på Facebook eller MSN, kan den fanges opp over *nettverksforbindelsen* som *elektronisk kommunikasjon*. Dette er viktig fordi sanntidskommunikasjon normalt ikke lagres og praktisk sett ikke kan sikres ved beslag i etterkant. Men hva konsekvensene blir dersom politiet for eksempel fanger opp "chat" når den *skrives* til datamaskinen (uhjemlet, ikke omfattet av hemmelig ransaking), i stedet for å fange den opp når den *sendes* over nettverksforbindelsen (hjemlet som kommunikasjonsavlytting), kan jeg ikke se at Metodekontrollutvalget har drøftet. Det reiser en problemstilling om ulovlig ervervet bevis, hvor påtalemyndigheten kan risikere bevisavskjæring.

Som sikkerhet mot å trå feil og risikere bevisavskjæring er det nærliggende at politiet både vil begjære kommunikasjonsavlytting og hemmelig ransaking. Oppsplittingen av gjennomføringsmåten på to forskjellige bestemmelser synes derfor å være lite hensiktsmessig. Den danske løsningen utløser ikke slike problemer så løsningen fremstår som enklere å praktisere og kontrollere.

Det norske forslaget tar heller ikke *samspillet* mellom metoder *over tid* i betraktning. Metoder kan derfor ikke avpasses for å utfylle hverandre over tid. Når hjemmelen for kommunikasjonsavlytting ikke kan benyttes for å fange opp tilgangskoder som kan gi mulighet til å foreta hemmelig ransaking av datasystem, og tilgangskoder for å dekode datatrafikk ikke kan fanges opp i forbindelse med hemmelig ransaking, *tvinges* politiet til å begjære bruk av alle tvangsmidlene, samtidig. I stedet kunne politiet vurdert for eksempel om avlytting var tilstrekkelig, fordi man kanskje ville få fatt i kodenøkkelen for beslag. Kanskje kunne man deretter nøyd seg med å foreta *ordinær* ransaking og beslag fordi man alt hadde den nødvendige kodenøkkelen.

Dersom lovgiver sterkt begrenser hva slags informasjon som kan fanges opp innenfor den enkelte hjemmel, blir metodebruken lite smidig. Resultatet er ikke nødvendigvis mer skånsomt for mistenkte.

2.3.4 Dekryptering av data i et etterfølgende ordinært beslag

Krypterte lagrete data utgjør i seg selv et problem for politiet. Dataavlesing for å fange opp kodenøkkelen idet den skrives eller kopieres inn i dekodingsfeltet kan imidlertid være et tiltak for å løse problemet. Jeg kan ikke se at Metodekontrollutvalget går spesielt inn på dette. Utredningen kapittel 23 handler vesentlig om atkomsten til data *mens de produseres.*

Man kan se for seg to ulike kontekster for metoden:

Den ene gjelder ved hemmelig beslag i forlengelsen av hemmelig ransaking. Konteksten er i så fall metodebruk mot den alvorligste kriminaliteten og terrorhandlinger. Da kan vidtgående inngrep være legitimt. Siden inngrepet er vidtgående må meget strenge vilkår gjelde. Dette synes å ha vært konteksten for Metodekontrollutvalgets vurderinger.

Den andre konteksten tar som utgangspunkt at krypterte beslag er et hyppig forekommende problem som ikke bare knytter seg til den alvorligste kriminaliteten. Da blir problemstillingen om det bør gis adgang til å fange opp kodenøkkelen *for å forberede et etterfølgende ordinært databeslag*, noe har svært *lav* inngangsterskel. Ifølge straffeprosessloven§ 203 kan beslag tas dersom tingen

”antas å ha betydning som bevis”, sml. retsplejeloven § 802 stk. 1 som krever at det må foreligge rimelig grunn til mistanke om et lovbrudd som er undergitt offentlig påtale, og være grunn til å anta at gjenstanden (dataene) kan tjene som bevis. Selv om beslaget skjer i forbindelse med ordinær ransaking skjerpes ikke vilkårene vesentlig. Etter straffeprosessloven § 192 er det tilstrekkelig med ”skjellig grunn” til mistanke om en handling som kan medføre frihetsstraff, og at formålet er å søke etter bevis. I dansk rett har retsplejeloven § 794 lignende vilkår.

På denne bakgrunn kan det reises spørsmål om det er mulig å utføre dataavlesing *i helt begrenset form utelukkende for å fange opp kodenøkkelen* med tanke på et senere *ordinært* beslag. Politiet kan ha behov for å gå frem slik på grunn av erfaring med at kryptering hyppig brukes i spesielle kriminelle miljøer. Hvis fremgangsmåten er praktisk mulig, er inngrepet mindre enn dataavlesing i ubegrenset form. Inngangsterskelen kan dermed være lavere. Metodekontrollutvalget synes å ha operert i den første konteksten, og har ikke behandlet dette spørsmålet. På den annen side forutsetter utvalget at metodebruken kan innrettes med presisjon for å fange opp kodenøkler, noe som nettopp er en forutsetning for den problemstilling jeg har reist.

Et eksempel kan illustrere krypterintgsproblemet: Ved et forskningseksperiment i Sveits i 2007 prøvde man å knekke en 700 bits kryptering ved et såkalt ”brute force attack ” (”brute force” er ”rå kraft”, dvs. at datamaskinen tester tilfeldige tegnkombinasjoner for å prøve å finne kodenøkkelen). Dette krevde innsatsen til 400 datamaskiner i 11 måneder. I dag er vanlig kommersielt krypteringsnivå nesten dobbel styrke. Uten kodenøkkelen er innholdet derfor praktisk sett utilgjengelig for politiet.[13] Kryptering representerer således en effektiv og enkelt anvendelig hindring for etterforsking av mange typer kriminalitet.

For ordens skyld kan det nevnes at den adgang politiet har etter straffeprosessloven § 199a, til å *”pålegge enhver som har befatning med datasystemet å gi nødvendige opplysninger for å gi tilgang til datasystemet”,* ikke løser problemet. Bestemmelsen er saklig avgrenset til opplysninger som kan gi *tilgang* til datasystemet (brukernavn og passord), og omfatter ikke kodenøkler som dekrypterer innholdet.[14]

3. Fremgangsmåter for å skaffe tilgang til opplysninger i et datasystem

3.1 Innledning

Her gis en oversikt over noen fremgangsmåter for å skaffe tilgang til opplysninger i et datasystem. Den faktiske kartleggingen gir bakgrunn for de etterfølgende drøftelsene.

Jeg skiller mellom ”utstyrs”- og ”informasjonsbaserte” fremgangsmåter. Betegnelsene er ikke rettslige. De tjener systematiske formål og letter den pedagogiske siden av fremstillingen. Det er hele tiden underforstått at tilgangen skjer hemmelig uten tillatelse fra innehaver (mistenkte).

[13] Sunde (2011) kap. 11.2 s. 209. Se også Datakrimutvalget NOU 2007: 2 kap. 3.4.7 om fremgangsmåter for å knekke kryptering.

[14] Ot.prp. nr. 40 (2004-2005) s. 29: ”Opplysningsplikten bør med andre ord begrenses til det som er nødvendig for å gi tilgang til det aktuelle datasystemet, for eksempel i form av tilgangskoder.” sml. s. 35.

3.2 Utstyrsbaserte fremgangsmåter

Utstyrsbaserte fremgangsmåter for å fange data opp fra et datasystem omfatter teknisk registrering av stråling, bruk av hardware og bruk av software (dataprogram).[15]

Stråling fra skjerm, tastatur og kabel kan registreres ved bruk av teknologi som kalles EMSEC eller TEMPEST. Bearbeidelse av signalene til lesbar informasjon er krevende og teknologien som er utviklet for militære formål, er i liten grad tilgjengeliggjort i politiet. Per i dag fremstår ikke fremgangsmåten som særlig praktisk for politiet, men det kan jo tenkes å endre seg med tiden. Beslektete varianter er mekanisk tilegnelse av avtrykk av tastetrykk og skjult fotografering av tastetrykk. Dette er velkjente metoder for å avsløre PIN-koder til bankkort. Alle måtene kan sies å gå ut på å fange opp data fra en datamaskin "ved tekniske midler", sml. uttrykket i retsplejeloven§ 791 b.

EMSEC er acronym for "Emanating Security". TEMPEST er akronym for følgende to uttrykk: "Telecommunications Electronics Material Protected from Emanating Spurious Transmissions" og "Transient ElectroMagnetic Pulse Emanation STandard".[16]

For det annet kan informasjon skaffes ved bruk av utstyr som *kopierer innhold* på datamaskinen ("kildedata"). Da betyr "avlesing" ordinær kopiering. Kopien er utbyttet av fremgangsmåten og representerer beviset. Både hardware- og software kan brukes. I begge tilfeller er teknologien lett tilgjengelig og koster lite.[17]

Den *hardwarebaserte* fremgangsmåten går ut på å montere en fysisk innretning på datamaskinen eller på linjen ut til omverdenen. Innretningen settes for eksempel på tastaturkabelen (og ser ut som en del av denne) eller festes som en minnepinne på en USB-port. Fordi utstyret er fysisk må det settes på en bestemt datamaskin og kan ikke utnyttes direkte mot brukerkonti i nettet. Denne begrensningen gjelder også strålingsalternativet. Den fysiske innretningen blir på norsk kalt "tastetrykksavleser" etter det engelske ordet "keylogger".[18] Dersom innretningen settes på tastaturkabelen kan den fange opp passord som skrives idet man logger seg på datamaskinen, åpner en tilgangskontrollert tjeneste eller en kryptert fil. Motsatt fanger den også opp passord som skrives idet en fil krypteres.

En fysisk innretning kan også ha funksjonalitet for å kopiere lagrete data og tappe trafikk ut/inn over nettverksforbindelsen. Da er det ikke naturlig å omtale den som "tastetrykksavleser". Snarere er den en generell "kopieringsinnretning". Også en tastetrykksavleser er en kopieringsinnretning, men med begrenset funksjonalitet.

Ved en *softwarebasert* fremgangsmåte installeres et dataprogram på mistenktes datamaskin eller brukerkonto i nettet. Programmet forholder seg til et logisk avgrenset område, dvs. et brukerområde / hjemmeområde uavhengig om det fyller en lokal datamaskin eller er ett av flere områder på en server. Programmet kan kopiere og sende data til politiet.

---

[15] Se for eksempel Wikipedia som på stikkordet "Keystroke logging" nevner "hard- and software based keyloggers" og "optical surveillance". Se også "Trojan horse" og "Packet analyzer". http://en.wikipedia.org/wiki/Keylogging (besøkt 12.11.2010).

[16] http://encyclopedia2.thefreedictionary.com/TEMPEST (besøkt 12.11.2010).

[17] Leseren kan sjekke dette ved å søke på nettet. Jeg synes ikke at jeg bør sette inn aktuelle nettreferanser fordi de er produsentspesifikke og jeg dessuten mangler grunnlag for å ha en oppfatning om de konkrete produktenes effektivitet.

[18] Metodekontrollutvalget beskriver dette på s. 248 i NOU 2009: 15. Se også Datakrimutvalget om "keylogger" i NOU 2007: 2 ss. 26 og 160.

I teknisk fagspråk kalles et slikt program ”*trojaner*”. Det anses som et ”hackerverktøy” (”exploit” eller ”malware”) når det er i feil hender.[19] I dansk rett er det omtalt som et ”snifferprogram”.[20] I forbindelse med dataavlesing velger jeg å kalle det ”politiprogram”, eventuelt ”polititrojaner”. Språkbruken markerer at det er *politiet* som installerer og utnytter programmet.

Normalt foregår installering og bruk av programmet over nett, men det kan også installeres ved at politiet skaffer seg fysisk adgang til datamaskinen. Bruk av polititrojaner kan effektivisere politiets arbeidsmåte. Politiet kan la programmet virke på mistenktes datamaskin / brukerområde i den tillatte periode uten at etterforskeren må være tilstede. I stedet kan man nøye seg med stikkprøver, eventuelt jevnlig kontroll av resultatet. Programmet kan også *varsle* om aktivitet av interesse, for eksempel dersom navn på bestemte personer skrives til datasystemet.

3.3 Informasjonsbaserte fremgangsmåter

Informasjonsbaserte fremgangsmåter for å skaffe tilgang til et datasystem krever ikke bruk av teknisk utstyr (annet enn tilgang til datasystem). De går ut på utnyttelse av brukernavn og passord (tilgangsdata) og av teknisk ”hackerkompetanse”.

Bruk av mistenktes brukernavn og passord innebærer at tilgang oppnås ved bruk av *ordinær påloggingsprosedyre* (bortsett fra at politiet ikke er rette innehaver av tilgangsdataene). Politiet får samme rådighet over datamaskinen / brukerkontoen som mistenkte selv har.

Bruk av ”hackerkompetanse” innebærer at politiet benytter teknisk ”know how” om *sårbarheter i programvaren* til å trenge seg inn ”bakveien”. I samsvar med Datakrimutvalgets språkbruk kaller jeg datainnbrudd ved pålogging for ”passordinbrudd” og inntrengning bakveien for ”sårbarhetsinnbrudd”.[21] I begge tilfeller er tilgangen til mistenktes datasystem *tidsmessig synkron* med at politiet trenger seg inn, undersøker, kopierer og går ut igjen. Dette er forskjellig fra bruk av polititrojaner.

3.4 Mellomformer

Man kan også tenke seg *mellomformer* som kombinerer utstyrs- og informasjonsbaserte fremgangsmåter, og utnytter sårbarheter forårsaket av andre enn politiet selv.

For det første kan politiet trenge seg inn via en sårbarhet i programutrustningen, for så å installere en polititrojaner. Da har man kombinert informasjons- og utstyrsbaserte fremgangsmåter.

Videre kan politiet utnytte en trojaner som oppdages på mistenktes datasystem. Dersom politiet hadde utplassert programmet selv, hadde det vært å anse som et politiprogram og fremgangsmåten ville vært utstyrsbasert. Men ved å utnytte en trojaner lagt inn av en annen, bruker politiet bare sin *kompetanse* til å avdekke en sårbarhet som gir mulighet for sårbarhetsinnbrudd. Kanskje kan politiet også gjøre trojaneren til ”sin” ved å overta kontrollen over programmet, noe som i så fall gjør metoden utstyrsbasert. Hvis politiet ikke gjør dette, men satser på at trojaneren er der også neste gang datamaskinen oppsøkes, er fremgangsmåten informasjonsbasert.

Eksemplet kan trekkes videre, for man kan tenke seg at politiet har avdekket trojaneren ved å bruke et dataprogram som søker etter kjente sårbarheter. I så fall brukes teknisk utstyr for *å finne*

---

[19] Datakrimutvalget beskriver ”exploits” og ”trojaner” i NOU 2007: 2 ss. 23-24.

[20] Gomard (2008) note 3 til retsplejeloven § 791 b. ”Sniffer program” er nevnt som eksempel på ”Packet analyzer”, jf. oppslaget på Wikipedia nevnt i tidligere note. Se også Metodekontrollutvalget ss. 247-248.

[21] NOU 2007: 2 ss. 22-23.

sårbarheten, mens *inntrengningen* skjer ved utnyttelse av kompetanse (informasjon). Maskinelle søk etter sårbarheter er en velkjent hackermetode.[22] Den kan brukes både mot en spesiell datamaskin (mistenktes) og bredt innen et spekter av IP-adresser (IP-adresse er vertsmaskinenes nettverksadresse).

Et eksempel finnes i Rt. 2004 s. 1619 (Bakdørsaken), hvor to menn ble domfelt for datainnbrudd og dataskadeverk mot flere hundre datamaskiner verden over. Fremgangsmåten for å finne servere som de kunne trenge inn i er av lagmannsretten beskrevet slik:

> De " « har begge forklart at de først brukte forskjellige skanneprogrammer som var installert på den datamaskin hackingen foregikk fra. Skanneprogrammet var programmert til å søke gjennom grupper av IPadresser, enten identifisert ved numrene eller domenenavn (...). Skanneprogrammet sender forespørsler til datamaskinene om de inneholder bestemte versjonsnumre av en type dataprogram. Når skanningen er fullført opprettes en logg som bl.a. viser hvilke datamaskiner som har den type program det har blitt søkt etter.
>
> Grunnen til at det ble søkt etter bestemte versjoner av programmer er at de tiltalte, ..., hadde funnet ut at enkelte versjoner av programmer inneholder svakheter. Svakhetene i programmer er for øvrig også offentlig kjent og publiseres på offentlig tilgjengelige internettsider (...).
>
> De svakheter i dataprogrammer som er omtalt ovenfor, kan utnyttes. Det finnes for en rekke svakheter utviklet såkalte exploitprogrammer - dataprogrammer som har som formål å utnytte svakheten, slik at man får tilgang til datamaskinen som kjører det aktuelle dataprogram. Ved å utnytte svakheten med en exploit omgås eieren av datasystemets forsøk på å beskytte tilgangen til datasystemet ved å kreve autentisering av brukeren med brukernavn og passord.
>
> Etter en vellykket kjøring av en exploit, er følgen at gjerningsmannen får tilgang som sk. rootbruker (systembrukeren med alle rettigheter til for eksempel å lese, endre eller slette filer samt installasjon av programmer og brukere) på den angrepne datamaskin.
>
> De tiltalte har i retten forklart at de har hatt og brukt forskjellige typer exploits, som har rettet seg mot ulike svakheter de har skannet etter. Fremgangsmåten for å komme seg inn i det angrepne datasystem har imidlertid i alle tilfellene vært som beskrevet ovenfor. »" (Rt. 2004 s. 1619 avsnitt 16).

Uttrykket "exploit" kan både betegne en *sårbarhet* i det datasystem som er under angrep, og det *hackerverktøy* (dataprogram) som brukes for å utnytte sårbarheten.[23] I forhold til dataavlesing mener jeg det er et poeng å holde klart for seg om man taler om en *eksisterende sårbarhet* på mistenktes datasystem, eller den sårbarhet som oppstår som følge av *implementering av et politiprogram* på datamaskinen. Politiet kan disponere et sett egne politiprogrammer spesielt utviklet for bruk på forskjellige operativsystem. Eksisterende sårbarheter kan på den annen side være en ordinær programsvakhet som politiet utnytter med sin "hackerkompetanse", eller en trojaner utplassert av tredjemann som politiet finner formålstjenlig å bruke.

---

[22] Datakrimutvalget kaller fremgangsmåten "elektronisk kartlegging i form av skanning", se redegjørelse NOU 2007: 2 ss. 24-25.

[23] Datakrimutvalget presiserer at "uttrykket ‹‹exploit›› [benyttes] både om metoden og programmet som anvendes", se NOU 2007: 2 s. 23 spalte 1.

4. En vurdering av Metodekontrollutvalgets forslag

4.1 Forslaget åpner ikke for vedvarende overvåking av et datasystem

Etter min mening hefter det flere svakheter ved Metodekontrollutvalgets forslag. Problemene kommer i tillegg til svakhetene ved den lovtekniske løsning som er kommentert i kapittel 2.3.3.

Et hovedproblem gjelder uklarheter med hensyn til hva metoden kan gå ut på. Utvalgets presisering av at det ikke åpnes for vedvarende overvåking av et datasystem står i et spenningsforhold til de fremgangsmåter som utvalget beskriver. På sidene 247-248 redegjør utvalget for adgangen til å bruke både et dataprogram og en fysisk tastetrykksavleser til å gjennomføre primærmetodene. Men disse fremgangsmåtene er nettopp varige i sin karakter. Bruk av polititrojaner og tastetrykksavleser åpner for vedvarende overvåking. Overvåkingen løper fra utstyret installeres til det avinstalleres.

Spenningsforholdet blir særlig tydelig i forhold til hemmelig ransaking, som til forskjell fra kommunikasjonsavlytting er strengt avgrenset i tid. Metodekontrollutvalget legger til grunn at politiet i medhold av en og samme ransakingstillatelse kan forsøke alternative atkomstmåter til ransakingsobjektet.[24] Men når ransakingen først er innledet må den avsluttes når objektet er ferdig gjennomsøkt. Ransaking gir ikke adgang til å bli værende på ransakingsstedet fysisk, eller ved følge med på det over tid ved hjelp av et dataprogram, med en tastetrykksavleser, eller for den del ved å registrere stråling, som redegjort for i kapittel 3. Siden norsk lov ikke åpner for gjentatt ransaking (dvs. flere ransakinger innen et spesifisert tidsrom) må politiet begjære ny ransakingsbeslutning dersom det er aktuelt å sikre bevis fra ransakingsobjektet på nytt.

Ved hemmelig ransaking av datasystem er det de *informasjonsbaserte atkomstmuligheter* som er aktuelle, siden disse ikke gir politiet noen vedvarende rådighet over ransakingsobjektet. Det er altså tale om passord- eller sårbarhetsinnbrudd (se kapittel 3.3). Slik atkomst til datasystem rammes som datainnbrudd, noe utvalget har formulert adgang til, jf. "å foreta innbrudd i et datasystem".

Selve den *tidsavgrensede karakter* som preger ransaking som metode, utelukker bruk av polititrojaner og tastetrykksavleser. I den forbindelse kan det også minnes om at dette ikke er de eneste fremgangsmåter som utvalget ser for seg. Utvalget finner at det "neppe er hensiktsmessig eller mulig" i detalj " å beskrive de fremgangsmåter som forslaget tar sikte på å gi adgang til, blant annet fordi en slik beskrivelse "raskt blir utdatert".[25] Utvalget ønsker imidlertid å sikre at hjemmelsgrunnlaget åpner for de måter å gjennomføre et tvangsmiddel på som er ønskelig.[26] Det opplyses at siden datainnbrudd er straffbart, jf. straffeloven 1902 § 145 annet ledd, må det gis eksplisitt hjemmel for denne fremgangsmåten.[27]

Men utvalget oppnår ikke å realisere sitt formål, fordi adgangen til å begå datainnbrudd *ikke* hjemler adgang til å installere en polititrojaner. Installering av et fremmed dataprogram regnes som en

---

[24] NOU 2009: 15 s. 246, langt ned i spalte 2.
[25] NOU 2009: 15 s. 247.
[26] NOU 2009: 15 s. 244.
[27] NOU 2009: 15 s. 245. Utvalget nevner ikke *lex superior prinsippet*, kun legalitetsprinsippet. Begrunnelsesmåten kan jo være en diskusjon for seg, Se i nyere norsk teori Høgberg/ Kinander (2011) om det materielle legalitetsprinsippet og dets begrunnelse. Stub (2011) diskuterer de to prinsippene i forhold til beslag som rettslig beslutning og faktisk handling. For mitt formål er det ikke nødvendig å gå inn på begrunnelsesmåten. Det er tilstrekkelig å vise til at dersom en handling er forbudt, må den eksplisitt tillates dersom politiet skal kunne benytte den. Dette gjelder uavhengig av om den omfattes av legalitetsprinsippet.

endring i programoppsettet på datamaskinen. En trojaner gir mulighet for gjentatt inntrengning i datasystemet, som en "bakdør" innehaveren av datasystemet ikke er klar over og ikke kan sikre seg mot. Fra innehaverens ståsted representerer bakdøren en sikkerhetssvikt. Selv om den ikke nødvendigvis rammer datasystemets funksjonalitet innebærer den at uvedkommende blant annet kan tappe systemet for informasjon. Dette regnes som dataskadeverk og rammes av den ordinære skadeverksbestemmelsen i straffeloven 1902 § 291. Bestemmelsen rammer "den som rettsstridig …skader … en gjenstand". Avgjørelsene i Rt. 2004 s. 94 og 1619 gir uttrykk for denne lovforståelsen.[28]

Atkomsten og tappingen (kopieringen) av data rammes som *uberettiget adgang til data,* jf. straffeloven 1902 § 145 annet ledd. Etter en lovendring i 2005 krever ikke loven lenger at den uberettigete adgangen skaffes ved "å bryte en beskyttelse", som er bakgrunnen for uttrykket "datainnbrudd".[29] Loven selv bruker ikke uttrykket. Det betyr at uberettiget adgang til data kan skje ved alle de utstyrs- og informasjonsbaserte fremgangsmåter som er beskrevet i kapittel 3, dvs. registrering av stråling, bruk av trojaner og tastetrykksavleser, samt kopiering av data i forbindelse med sårbarhets- og passordinnbrudd.[30] I *resultatet* korresponderer det strafferettslige forbudet mot uberettiget adgang til data med dataavlesing som selvstendig metode. Kombinert med en adgang til å installere en polititrojaner på systemet ville det norske forslaget fullt ut korrespondert med den danske løsningen i retsplejeloven § 791 b.

Men dette resultatet har ikke Metodekontrollutvalget ønsket. Likevel har utvalget ønsket å tillate bruk av polititrojaner. Disse ønskene later ikke til å la seg forene. En sak for seg er at den *lovtekniske* løsningen er utilstrekkelig med tanke på dataskadeverket. Da måtte utvalget i tillegg ha foreslått en adgang til å installere et dataprogram, jf. *lex superior prinsippet*.

Uansett er det tilbakevendende problem er at den hemmelige ransakingen ikke skal være vedvarende. Slik utvalget har formulert forslaget kan politiet ikke gå frem slik utvalget uttrykkelig beskriver. For bruk av polititrojaner ville det være et lovbrudd, jf. straffeloven 1902 § 291. Og både for polititrojaneren og de øvrige utstyrsbaserte atkomstmåter ville det stride mot ransaking som tidsavgrenset metode. Politiet vil bare ha uttalelser i forarbeidene som bryter mot metodens karakter, som hjemmel for fremgangsmåten. Det må i beste fall må sies å gi en svak og usikker hjemmel.

Så kan man til støtte for forslaget innvende at Metodekontrollutvalget klart har tatt mål av seg å imøtekomme politiets behov for å håndtere krypteringsproblemet. Generelt er lovens formål et relevant tolkingsmoment. Dets vekt avhenger både av forholdet til andre tolkingsmomenter, og hvor klart formålet lar seg utlede. I dette tilfellet står formålet om å avhjelpe krypteringsproblemet imot klar uttalelse om at det ikke åpnes for overvåking av vedvarende karakter, noe som nettopp er nødvendig for å realisere formålet.

Videre kompliseres bildet av begrensningen med hensyn til hvilke data som kan fanges opp med hjemmel i de respektive bestemmelser (se kapittel 2). For eksempel ville det lette politiets

[28] Avgjørelsene er beskrevet og analysert i Sunde (2006) ss. 195-197.
[29] Endringslov 8. april. 2005 nr. 16.
[30] Oppfanging av stråling er kanskje ikke så strekt vektlagt i forbindelse med forståelsen av innholdet i straffeloven § 145 annet ledd, men at det omfattes synes å være hevet over tvil. Det følger som en forpliktelse av Europarådets konvensjon mot datakriminalitet (ETS 185) artikkel 3 og er omtalt i beskrivelsen av gjeldende rett av Datakrimutvalget i NOU 2003: 27 kapittel 2.3.

muligheter for hemmelig ransaking å få fatt i brukernavn og passord til datasystemet. Men disse kan ikke benyttes dersom de er fanget opp i forbindelse med kommunikasjonsavlytting. For å kunne bruke opplysningene må de være fanget opp i forbindelse med ransaking, men da er jo også behovet for å få fatt i opplysningene bortfalt. Så hvordan Metodekontrollutvalget egentlig har tenkt at bestemmelsene skal brukes fremstår som uklart.

4.2 Adgangen til å ransake over nett

Metodekontrollutvalget ønsker også å åpne for ransaking av datasystem over nett. Problemstillingen er formulert som et spørsmål om ransaking forutsetter "politiets fysiske tilstedeværelse".[31] Metodekontrollutvalget opplyser at tillatelse til ransaking over nett har vært gitt i tingrettspraksis, noe som etter gjeldende rett savner en "klar rettskildemessig forankring".[32] Som nevnt ser utvalget ser behovet for fremgangsmåten og ønsker med tilføyelsen av adgangen til å foreta innbrudd i datasystem å presisere loven slik at den klart hjemler ransaking over nett.

Dette er imidlertid ikke helt enkelt å lese ut av lovteksten etter endringen.

For det første kan man ikke av en adgang til å foreta datainnbrudd utlede at det gis adgang til å foreta dette uten fysisk nærvær, dersom det rettslige utgangspunktet først er slik at at ransaking krever fysisk nærvær. Hovedbestemmelsen om ransaking er straffeprosessloven § 192 første ledd hvoretter ransakingsobjektene er definert som "bolig, rom eller oppbevaringssted". Bestemmelsen om hemmelig ransaking bygger på denne og tilføyer at metoden på strenge vilkår kan brukes med utsatt eller helt unnlatt underretning. Siden det er langvarig praksis for at datasystem kan ransakes med hjemmel i den ordinære ransakingsbestemmelsen i straffeprosessloven § 192 første ledd, kan dette selvsagt også gjøres som hemmelig metode.

Også ved ordinær ransaking kan politiet være tvunget til å begå datainnbrudd dersom datasystemet på ransakingsstedet er slått av eller brukeren er avlogget. Det er datainnbrudd *med fysisk nærvær*. Man har basert seg på straffeprosessloven § 200 siste ledd annet og tredje punkt som bestemmer at "om nødvendig kan det åpnes adgang med makt. Det som er brutt opp skal så vidt mulig lukkes til etter ransakingen." Når det først foreligger rettslig aksept for at logisk gjennomsøking av datasystem er å regne for ordinær ransaking, jf. § 192, er det nærliggende at siste leddet i § 200 anses som tilstrekkelig hjemmel for å begå datainnbrudd. Begge bestemmelsene er i utgangspunktet utferdiget med tanke på fysiske forhold. Når "rom" i § 192 fortolkes slik at datasystem omfattes, burde ikke adgangen til å åpne datasystemet med makt, utelukke at politiet skaffer seg adgang ved alminnelig pålogging. Politiet kan jo finne påloggingsdata som er nedskrevet på en gul lapp som er gjemt vekk i en skuff. Påloggingen er datainnbrudd, koherenshensyn tilsier at fremgangsmåten omfattes av § 200.

Det hører med i bildet at straffeprosessloven har blitt supplert med § 199a, som nettopp tar utgangspunkt i at datasystem som skal ransakes kan være utilgjengelig for politiet.[33] Ifølge bestemmelsen kan politiet "pålegge enhver som har befatning med datasystemet å gi nødvendige opplysninger for å gi tilgang til datasystemet". Men også uavhengig av denne bestemmelsen har nok ransakingsreglene vært forstått slik at politiet har kunnet prøve forskjellige passordmuligheter m.v., for å oppnå tilgangen.

---

[31] NOU 2009: 15 s. 246.
[32] NOU 2009: 15 s. 246.
[33] Tilføyd ved lov 8. april 2005 nr. 16.

På denne bakgrunn kan man spørre om tilføyelsen av adgangen til å foreta datainnbrudd for å effektivisere hemmelig ransaking i det hele tatt var nødvendig.

I forhold til å presisere adgangen til å ransake over nett synes det å ha større betydning hvordan man skal forstå uttrykket ”datasystem” i straffeprosessloven § 200a siste punktum ledd. Innebærer det at ransaking over nett bare omfatter datasystemer som under en ordinær ransaking ville vært fysisk tilgjengelige for politiet? Eller omfattes også mistenktes brukerkonti i nettet, som vanligvis er utenfor politiets fysiske rekkevidde fordi de ligger på servere tilhørende elektroniske tjenesteytere?

Dersom Metodekontrollutvalget mente å åpne for ransaking av brukerkonti i nettet, burde ordet ”brukerkonto” vært nevnt i lovteksten. Politiet har et praktisk behov for å gå frem på denne måten, siden brukerkonti i ”internettskyen” blir stadig viktigere som lagringsplass for data.

Dersom forslaget blir gjennomført slik det nå står, vil det fortsatt herske tvil på et område som har vært diskutert i utredninger i hvert fall siden Metodeutvalgets utredning i 1997.[34] Ransaking over nett forutsetter at ransakingsobjektet er et elektronisk kommunikasjonsanlegg. Fortolkningen av ”datasystem” i straffeprosessloven § 200a siste punktum (hemmelig ransaking) bør derfor være den samme som ”datasystem” i straffeprosessloven § 216a fjerde ledd (om datainnbrudd i forbindelse med kommunikasjonsavlytting). For sammenhengens skyld må det antas at man skal legge til grunn gjeldende fortolkning av uttrykket ”anlegg for elektronisk kommunikasjon” som er benyttet i bestemmelsen om kommunikasjonsavlytting tredje ledd. Uttrykket angir hva slags objekt kommunikasjonsavlytting kan rette seg mot.

I en oppsummering av gjeldende rett i tilknytning til uttrykket ”anlegg for elektronisk kommunikasjon” sier Metodekontrollutvalget at ”anlegget må … identifiseres i rettens kjennelse”.[35] Deretter nevnes fasttelefon, telefaks, mobiltelefon, ”datamaskiner i nettverk” og hjemmemaskiner. Det eneste eksemplet som kan tenkes å omfatte brukerkonti i nettet er ”datamaskiner i nettverk”, men brukerkonti er ikke nevnt, og alle de øvrige eksemplene gjelder fysisk utstyr. Det gir knapt holdepunkt for at brukerkonti i nettet er omfattet.

Situasjonen synes å være den samme i Danmark. Bestemmelsen om dataavlesing bruker ordet ”informationssystem”, og i beskrivelsen av hva det betyr sier lovkommentaren

”informationssystemet kan i givet fald identificeres ved den adresse, hvor det benyttes, eller – for bærbart udstyr – ved angivelse af den person, der har rådighed over udstyret.”[36]

Sml. Smith (2011) som skriver at kjennelsen skal angi ”hvilken computer eller lignende databehandlingsanlæg, indgrebet skal angå”, og nevne ”det geografiske sted” m.v..[37]

Se også Smith (2011) s. 455 nederst. Det opplyses at med ”et informationssystem forstås en computer eller andet databehandlingsanlæg. Omfattet heraf er navnlig personlige computere, herunder både stationære og bærbare computere. Også andet elektronisk utstyr vil imidlertid kunne være omfattet af bestemmelsen, hvis udstyret har funktioner svarende til dem, der findes i personlige computere … for eksempel en elektronisk

[34] NOU 1997: 15 kapittel 4.2.1.3 ”Om datanettverk” ss. 57 flg.
[35] NOU 2009: 15 s. 176.
[36] Gomard (2008) note 9 til retsplejeloven § 791b.
[37] Smith (2011) s. 456.

kalender, som … kan anvendes til at sende og modtage elektroniske meddelelser samt indhente oplysninger fra internettet mv.".

Alt i alt gis det lite veiledning for så vidt gjelder adgangen til å foreta ransaking mot brukerkonti i nettet. Det har også hersket motforestillinger mot en slik adgang, særlig på grunn av jurisdiksjonsproblemer. Det kan være en grunn til at man ikke tydelig har åpnet for fremgangsmåten.

Men som en konklusjon på drøftelsen av adgangen til å ransake over nett, må det også her fastslås at Metodekontrollutvalgets forslag ikke er særlig avklarende, og at lovteksten med den endring som er foreslått vel heller ikke gir tydelig anvisning på fremgangsmåten.

5. Om dataransaking bør skilles ut av reglene om fysisk ransaking

I arbeidet med denne analysen er jeg kommet til at lovgiver burde vurdere å skille ut reglene om dataransaking fra reglene om fysisk ransaking. Mange grunner taler for det. Jeg nevner at situasjonene er svært forskjellige; at forskjellen har betydning for vurderingen av hvor inngripende metodene må anses for å være; og at utskilling kan bidra til å unngå et uheldig press på ransakingsreglene.

Dataavlesing har en side både mot kommunikasjonsavlytting, hemmelig ransaking og beslag. Den tradisjonelle inndelingen av metodene er basert på om de retter seg mot data under overføring (avlytting) eller data som er lagret (ransaking og beslag). Behovet for dataavlesing oppstår fordi denne inndelingen er blitt for rigid i forhold til utviklingen av ekomtjenester og brukeratferd. Bruken av kryptering er bare et alminnelig utviklingstrekk i dette bildet. Behovet for vedvarende overvåking av mistenktes datasystem og brukerkonto i nettet, har også andre årsaker. Etter mitt syn gir det grunn til å vurdere behovet for å endre den straffeprosessuelle lovgivningen slik at den bedre samsvarer med tekniske og sosiale utviklingstrekk.

For det første er det ikke lenger slik som i fasttelefonens dager at kommunikasjon nødvendigvis skjer mellom forskjellige parter, ei heller at kommunikasjon nødvendigvis kan fanges opp i det den overføres. Dette ser man når man skiller mellom *teknisk* og *sosial* kommunikasjon. Det er også relevant at ekomtjenester i dag i stor utstrekning er bygd opp rundt *personlige brukerkonti og kommunikasjonsadresser*. Det er vanlig at hvert individ disponerer sin individuelle kommunikasjonsadresse og brukerkonto. Dette gjelder også innen familien, hvor både barn og foreldre har egen mobiltelefon og epostadresse.

Med utgangspunkt i mobilen kan mistenkte kontakte sin egen brukerkonto (epostkonto, google docs. m.v.). I *teknisk* forstand er dette *kommunikasjon* på grunn av den elektroniske overføringen av signaler, jf. ekomloven § 1-5 nr. 1 som sier at "elektronisk kommunikasjon" er "overføring av lyd, tekst, bilder eller andre data ved hjelp av elektromagnetiske signaler i fritt rom eller kabel i et system for signaltransport." 'Kommunikasjon' er da et rent teknisk begrep som står i motsetning til 'data som er lagret'.

Ved vedtakelsen av ekomloven 4. juli 2003 nr. 83 ble flere bestemmelser i straffeprosessloven endret for å inkorporere ekomlovens definisjon av "elektronisk kommunikasjon" i straffeprosessloven.

Formålet var å gjøre reglene teknologinøytrale. Dette gjaldt straffeprosessloven §§ 118, 211 og 216a om kommunikasjonsavlytting.[38]

Problemet er imidlertid at reglene om kommunikasjonsavlytting er utformet under forutsetning om at det er tale om *sosial kommunikasjon*, dvs. kommunikasjon som involverer flere parter enn mistenkte. Denne forutsetningen slår ikke nødvendigvis lenger til og dermed oppstår anomalier i lovverket.

I eksemplet med å kontakte google-kontoen fra sin datamaskin er poenget nettopp at det *ikke* har skjedd noen kommunikasjon mellom personer. Situasjonen er reelt sett den samme som om mistenkte hadde brukt sin lokale datamaskin for å foreta noen nedtegnelser eller sjekke opplysninger. Oppfanging av aktivitet på lokal maskin er ikke kommunikasjonskontroll. Det burde ikke være relevant for bedømmelsen av politimetoden at en tilsvarende bruk skjer over nett. Bruk av hjemmelen for kommunikasjonsavlytting med strenge vilkår blant annet av hensyn til familien, passer ikke så godt fordi situasjonen er en annen enn den regelen er ment for.

Den andre siden av dette poenget er at sosial kommunikasjon mellom kriminelle *ikke* kan fanges opp ved kommunikasjonskontroll på linjen mellom tekniske endepunkter når informasjonsutvekslingen skjer på *en felles brukerkonto.* Det spiller ingen rolle hva slags tjeneste som benyttes, dvs. om det er en epostkonto eller en personlig konto for lagring av dokumenter (for eksempel google docs). Ved å dele brukernavn og passord kan hver deltaker i den kriminelle aktiviteten logge seg inn, se gjennom beskjedene og tilføye sine egne kommentarer. Denne informasjonsutvekslingen kan ikke avdekkes ved ordinær kommunikasjonskontroll fordi utnyttelsen av brukerkontoen ikke er bundet til noen spesifikk datamaskin eller kommunikasjonsadresse. Deltakerne kan koble seg opp via internettkafé, terminal på hotell, flyplass og andre offentlige steder, og således sette seg utenfor kommunikasjonskontrollens rekkevidde. Reglene om kommunikasjonskontroll gir ikke adgang til å overvåke en datamaskin eller brukerkonto, noe som ville vært nødvendig for å følge med på informasjonsutvekslingen. Det gjør heller ikke bestemmelsen om hemmelig ransaking, fordi ransaking ikke kan skje vedvarende.

Etter min mening tilsier utviklingen at reglene om hemmelig ransaking over nett og kommunikasjonsavlytting burde slås sammen til én bestemmelse, hvor sentrale kriteriet er at metodebruken kan *skje over tid* (er av vedvarende karakter) og rette seg mot *elektroniske data*. Bestemmelsen burde gi adgang til å fange opp elektronisk kommunikasjon, data som er lagret og data som skrives til systemet. Metoden er like inngripende som kommunikasjonsavlytting, hemmelig ransaking og dataavlesing, og må ha de samme inngangskriterier m.v..

Begrensninger i adgangen til å bruke tvangsmidler utenfor territoriet kan være et problem i nettet. Plassen tilsier ikke at jeg går inn på en nærmere drøftelse av jurisdiksjonsspørsmålet her. Jeg nøyer meg med å vise til at det kan være en relevant forskjell mellom passordinnbrudd og sårbarhetsinnbrudd. I det første tilfellet innebærer fremgangsmåten bruk av mistenktes virtuelle identitet, noe som ikke åpenbart leder til noe jurisdiksjonsproblem selv om brukerkontoen er registrert hos utenlandsk tilbyder. Noe annet kan være tilfelle ved sårbarhetsinnbrudd, fordi inntrengningen da kan ramme ekomtilbyderen (tredjeperson) ved at politiet utnytter en

[38] Sunde (2011) ss. 125-126 om teknologinøytralitet i straffeprosessloven.

sikkerhetssvikt på systemet. Da antar inngrepet en tydeligere karakter av å inntreffe utenfor territoriet, og kan anses å være i strid med jurisdiksjonsreglene.

Videre burde reglene om *dataransaking skilles ut fra reglene om fysisk ransaking*. De digitale og fysiske forholdene er forskjellige og hensyn slår ikke til på samme vis. Jeg mener dette burde gjelde all form for dataransaking uavhengig av om det skjer åpent eller skjult, mot en fysisk maskin eller en brukerkonto. En dataransakingsbestemmelse kan åpne for gjentatt ransaking uten at det leder til press på den *fysiske* ransakingsbestemmelsen hvor sterke mothensyn gjør seg gjeldende.

Både vedvarende og gjentatt ransaking av en bolig må antas å være langt mer inngripende, ikke minst for familiemedlemmer, enn overvåking av mistenktes personlige brukerkonto. Det sistnevnte inngrepet fremstår som langt mer begrenset. Behovet er også overbevisende i lys av de raske endringer som skjer i elektronisk kommunikasjon. Metodekontrollutvalgets innvending mot å tillate fortløpende ransaking er først og fremst begrunnet i hensynet til familien. Dette er det enkelt å slutte seg til når det gjelder tvangsmiddelbruk mot familiens bolig. Men som det fremgår slår ikke hensynet på samme måte til i den digitale dimensjonen. Uansett bør vurderingen høre under retten i en konkret forholdsmessighetsvurdering, jf. straffeprosessloven § 170a. Da kan en begjæring avslås dersom den gjelder en epostkonto som disponeres av familien i fellesskap og hensynene som taler for inngrepet ikke er tilstrekkelig tungtveiende.

Ytterligere synes det noe uheldig i forhold til hvordan man oppfatter ransaking som metode, om lovgiver oppgir kravet til *fysisk tilstedeværelse* i datasammenheng. Dermed kan det bli vanskelig å si hvor grensen for ransaking går og man risikerer å tape noe av den konseptuelle forståelsen av metodens innhold. Da er det for eksempel neppe ulogisk at også fjernsynsovervåking rettet mot private rom kan være ransaking.

I svensk rett har man reist flere spørsmål rundt elektronisk ransaking og beslag som går langt utover de som her er reist. Blant annet gjelder det spørsmål om kopiering av data kan regnes som beslag, om gjennomsøking av et datasystem som er tatt med til politistasjonen skal regnes som ransaking, hvordan plikten til å ha et vitne til ransaking i så fall skal oppfylles osv. Slike problemer finnes også i norsk og dansk rett til tross for en noe mer pragmatisk tilnærming som ikke har satt spørsmålene på spissen.

6. Rettssikkerhetsspørsmål

6.1 Rettssikkerhetsstandarden

Dataavlesing representerer et inngrep (”interference”) i mistenktes privatliv og korrespondanse, jf. EMK art 8.1 og representerer en krenkelse av disse rettighetene med mindre vilkårene som følger av EMK art. 8.2 er overholdt. Vilkårene gjelder krav til legitimt formål (oppfylt fordi kriminalitetsbekjempelse omfattes), at inngrepet har hjemmel i lov og er nødvendig i et demokratisk samfunn.

Hele artikkel 8 ”*Right to respect for private and family rights”* lyder slik (engelsk språkdrakt):

“8.1 Everyone has the right to respect for his private and family life, his home and his correspondence.

8.2 There shall be no interference by a public authority with the exercise of this right except such as in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.”

EMK er implementert i norsk, svensk og dansk intern rett. I det følgende skal jeg behandle noen rettssikkerhetsspørsmål som er spesielle for dataavlesing utført ved inntrengning i et datasystem. Det omfatter både bruk av polititrojaner og informasjonsbaserte inntrengningsmetoder.

Etter EMK art. 8 er det grunnleggende at rettssikkerheten bygger på lov. For så vidt gjelder skjult overvåking har menneskerettighetsdomstolen i Strasbourg (EMD) ved flere anledninger slått fast at det er

”essential to have clear detailed rules on the subject, especially as the technology for use is continually becoming more sophisticated.[39]

Begrunnelsen er hemmelig overvåking er vanskelig å kontrollere og derfor utgjør en trussel mot demokratiet.[40] Strenge betingelser gjelder uansett om overvåkingen er mistankebasert og retter seg mot bestemte individer, slik dataavlesing gjør, eller er såkalt ”strategisk overvåking” av generell karakter.[41]

EMD krever at det i formell lov angis ”minimum safeguards” som beskriver hvilke lovbrudd som kan gi grunnlag for metodebruken, hvem som kan tenkes å bli utsatt for den, angir en temporær begrensning og gir retningslinjer for undersøkelse, bruk og lagring av de data som anskaffes ved metoden. Loven skal også inneholde taushetsregler og regler om sikkerhetstiltak ved utveksling av data.[42] Jeg går ikke nærmere inn på disse vilkårene.

I tillegg kreves det at loven utpensler de mekanismer som er nødvendige for *å hindre misbruk og skape tillit til myndighetenes praktisering av inngrepsadgangen*. EMD krever dokumentasjon for at lovens kontrollmekanismer eksisterer og er tatt i bruk, slik at retten kan føle seg overbevist om at metoden praktiseres på betryggende måte. EMD har således uttalt at den må kunne si seg

”satisfied that there exist adequate and effective guarantees against abuse”.[43]

Om vilkåret er oppfylt må ifølge EMD avgjøres i lys av alle sakens omstendigheter (”all the circumstances of the case”). Denne totalvurderingen skal blant annet ta i betraktning

”the nature, scope and duration of the possible measures, the ground for ordering them, the authorities competent to permit, carry out and supervise them, and the kind of remedy provided by national law”.

Vilkårene er knesatt i formuleringer med lang tradisjon i EMDs praksis, helt tilbake til Klass v. Tyskland i 1978 (pkt. 50), og fra nyere tid: saken mot Bulgaria i 2008 om telefonovervåking

---

[39] Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria (2008) pkt. 75 med videre henvisninger. Formuleringen gjenfinnes hvertfall så tidlig som i Kruslin v. Frankrike (1990), se pkt. 33, og er gjentatt i overvåkingssakene deretter.

[40] Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria (2008) pkt. 75 med videre henvisninger. Se også Klass v. Tyskland (1978) pkt. 49 om at overvåkingslover “poses [danger]of undermining or even destroying democracy on the grounds of defending it”.

[41] I Liberty and Others v. Storbritannia (2008) pkt. 63 sier EMD at “The Court does not consider that there is any ground to apply different principles concerning the accessibility and clarity of the rules governing interception of individual communications, on the one hand, and more general programmes of surveillance, on the other.”

[42] Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria (2008) pkt. 76; Weber og Saravia v. Tyskland (2006) pkt. 95.

[43] Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria (2008) pkt. 77.

Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria (2008) pkt. 77. Vilkårene har preg av å være rettslige standarder som kan fange opp nye inngrepsformer muliggjort av ny teknologi. De gjelder derfor også dataavlesing ved bruk av trojaner selv om EMD ikke har uttalt seg konkret om denne metoden. Dette henger igjen sammen med at EMD betrakter konvensjonen som et "living instrument" som skal fortolkes i lys av sin tid, noe som reflekteres i EMDs formålsorienterte og dynamiske tolkingsstil.

Slik jeg forstår det søkes flere formål oppnådd med de nevnte tiltak. Formålene går ut på (i) å holde politiet i sjakk; (ii) å skape tiltro i befolkningen til at deres rettigheter respekteres; og (iii) sørge for at myndighetene kan holdes ansvarlig dersom ikke lovens rammer respekteres. Systemet bygger på symmetri i partsforholdet mellom stat og borger. Det betyr at borgernes aksept av rettighetsavståelse korresponderer med en forventning om å kunne holde staten ansvarlig for eventuelt misbruk. Uten effektiv mulighet for ansvarliggjøring faller mekanismen som holder myndighetene i sjakk og dermed også tilliten til systemet.

På den rettslige bakgrunn som her er skissert skal jeg drøfte om rettssikkerhetskrav tilsier at loven bør oppstille krav til det dataprogram som benyttes som polititrojaner og til etterforskernes kompetanse ved metoder som retter seg mot innsiden av mistenktes datamaskin.

6.2 Kompetansekrav – hensynet til bevistes integritet

Bruk av politiprogram skjer *på innsiden* av datamaskinen, i motsetning til oppfanging av stråling og bruk av hardware som skjer fra utsiden. Det samme gjelder når tilgang skaffes ved å utnytte brukernavn og passord eller "hackerkompetanse" (informasjonsbaserte metoder).

Dette har interesse i forhold til det prinsippet for bevissikring som gjelder vernet om bevisets integritet. Prinsippet gjelder generelt fordi det selvsagt er grunnleggende at ethvert bevis skal representere en form for sannhet. Det bør derfor være autentisk (opprinnelig). Dette kan utledes av kravene til objektivitet og kvalitet i etterforskingen, og formålet om å komme frem til en sann beskrivelse av det faktiske hendelsesforløpet, som blant annet straffeprosessloven § 294 er et uttrykk for. Bestemmelsen sier at retten av eget tiltak skal "våke over at saken blir fullstendig opplyst".

For elektronisk bevissikring er det et problem at ubeskyttede data er sårbare for endring og sletting. Retningslinjer for "beste praksis" går derfor ut på at etterforskingen så langt som mulig bør unngå å røre ved ubeskyttede data.

Dersom det er nødvendig å sikre bevis fra aktive datasystemer sørges det for å anvende verktøy som *blokkerer* etterforskerens mulighet for å foreta endringer. Da er dataene beskyttet og kan bare *kopieres*. Såfremt politiet kan dokumentere at dataene som presenteres som bevis i retten er eksakt kopi av dataene på ransakingsstedet/-tidspunktet, kan dataene anses å være autentiske.

Det kan vises til G8 anbefalingene om "digital evidence", inntatt i ENFSI "Guidelines for Best Practice in the Forensic Examination of Digital Technology" v.5 (2006), pkt. B og C. Punkt B gjelder integritetshensynet og punkt C forutsetter at tjenestepersonen er "suitably trained". Sml. ACPO Good Practice Guide for Computer based Electronic Evidence v 3.0 (2003), Principle 1 and 2. Det kan også vises til internasjonalt anerkjent litteratur, se Casey (2004) som nevner "Integrity" som selvstendig punkt i en "logical flow of events" som utgjør dataetterforsking (s. 103) og utdyper dette i kap. 4.2.5 om "preservation" (s. 108). Han presiserer at etterforskeren må "make sure that potentially volatile items remain unchanged" og at "proper actions must be

taken to ensure the integrity of potential evidence". Sml. Carrier (2010) s. 5 om "The System Preservation Phase" og ss. 59-60 om Integrity Hashes. Se også SWGDE "Data Integrity within Computer Forensics" (2006).

Ved bruk av polititrojaner, pålogging og "know how" kommer etterforskeren i posisjon både til å endre og slette data på mistenktes datamaskin. I verste fall kan det være tilsiktet, men slikt kan også skje uforvarende. Integritetshensynet må avveies mot andre hensyn. Hensynet må vike dersom man ellers ikke kan få tatt beviset. Det kan være tilfelle dersom data krypteres når et datasystem logges av. Da kan det være nødvendig å ta kopi av ubeskyttede data. Men integritetshensynet tilsier at bevissikring av ubeskyttede data skjer under særlig god kontroll.

Det er derfor nærliggende *å kreve at loven stiller formelle kompetansekrav til utførende etterforsker*, dvs. at dataavlesing bare kan gjøres av etterforsker som er trent og har spesiell tillatelse. Dette er mer viktig enn ved databeslag ellers, fordi dataavlesing er en hemmelig metode hvor kontrollproblemer gjør seg gjeldende. Lovgiver skaper et lite betryggende system om man betror tillit til enhver etterforsker med "hackerkompetanse" til å utføre metoden.

Videre kan man for eksempel tenke seg at trojanervarianten bare bør kunne utføres ved hjelp av *egenutviklet program* slik at politiet *kjenner og kan dokumentere alle egenskapene*. Det gir også bedre mulighet for å utøve reell etterfølgende kontroll, slik Kontrollutvalget har ansvaret for i Norge. I en artikkel om EOS-utvalgets virksomhet har Hernes (2009) påpekt kontrollproblemene ved elektronisk hemmelig metodebruk, dvs. parallelle problemstillinger.[44] Ved eventuell innføring av dataavlesing har lovgiver oppfordring til å stille relevante krav her. Behovet for bruk av egenutviklet program støttes også av risikoen for at trojaneren misbrukes av uvedkommende, som drøftes i neste kapittel.

6.3 Kontroll mot misbruk av tredjeperson

Spørsmålet som drøftes her er om bruk av polititrojaner over nett i det hele tatt er en metode som kan oppfylle den rettssikkerhetsstandarden som det er redegjort for. Den skal både være undergitt reell kontroll og det skal herske tillit til at den er betryggende kontrollert.

Bruk av polititrojaner synes nemlig å stå i en særstilling med tanke på risiko for misbruk. Som det fremgikk av Bakdørsaken (Rt. 2004 s. 1619) nevnt i kapittel 3, kan kjente trojanere (exploits) avdekkes ved automatiske søk på nettet. Dette gjelder også polititrojanere. Dersom politiet bruker alminnelig kommersielt tilgjengelig programvare for å utføre dataavlesing vil andre nødvendigvis ha kjennskap til polititrojanerne og kunne søke etter og misbruke dem.

Kanskje vegrer politiet seg for å bruke slik teknologi, og benytter i stedet teknologi som er spesielt utviklet med tanke på politiets behov. Slik teknologi utvikles innenfor myndighetenes egne organisasjoner, innen politiet, sikkerhetstjenesten eller andre "high tech units" som for eksempel National Security Agency i USA, og i visse kommersielle bedrifter etter avtale med myndighetene (på samme vis som våpenindustrien).

Internasjonalt finnes det et marked for teknologi til politiet. Ofte deles dataprogrammer utviklet innenfor en organisasjon med andre tilsvarende organisasjoner på vilkår om at teknologien ikke gjøres alminnelig kjent. Resultatet er uansett at "law enforcement" organisasjoner verden over

[44] Hernes (2010) ss. 318-320. EOS-utvalget er Stortingets kontrollutvalg for etterretnings-, overvåkings- og sikkerhetstjenestene.

kjenner til hverandres teknologi. For noen kan man tenke seg at teknologideling er motivert av ønske om å oppnå innsikt i andre myndigheters metodebruk, for derigjennom å skape økte muligheter i ens egen etterforskings- og etterretningsvirksomhet.

Det er *nettverksteknologien* og det *asymmetriske trusselbildet* som tilsier at denne risikoen fortjener oppmerksomhet. På grunn av fremveksten av terror og grov grenseoverskridende kriminalitet anses kriminelle individer utenfor landets grenser som trusler mot landet selv. Internasjonalt opprettede lister definerer individer som terrorister som det er en global fellesoppgave å ramme. Det gjør dem interessante og sårbare for inngrep fra "law enforcement" i mange land, uavhengig av hvor individet konkret er bosatt eller oppholder seg.

Som illustrert av Bakdørsaken er disse individenes kommunikasjonsutstyr og brukerkonti tilgjengelige for "law enforcement" verden over via nettverksteknologien. Det betyr at politiet ved installering av polititrojaneren skaper *en allment tilgjengelig sårbarhet* på mistenktes datamaskin. I lys av det nevnte risikobildet kan neppe muligheten utelukkes for at sårbarheten kan bli forsøkt utnyttet av andre. Det representerer en meget betenkelig risiko ved fremgangsmåten.

Problemstillingen kan også tenkes å ha aktualitet for andre metoder som innebærer utplassering av politisendere m.v.. For eksempel er det tenkelig at uvedkommende kan fange opp signaler fra en politisender som brukes ved teknisk sporing. Man kan også tenke seg at en hardwarekomponent som settes på mistenktes datamaskin, er utstyrt med en sender som overfører signalene til politiets mottaker. I slike tilfelle oppstår det spørsmål om å skjerme signalene for bruk fra andre. Et alternativ for keyloggermetoden er at signalene lagres på den fysiske innretningen uten videresending, slik at politiet må skaffe seg innretningen tilbake for å kunne nyttiggjøre seg dataene.

Spørsmålet er om risikoen ved bruk av trojaner medfører at loven må oppstille spesielle vilkår for å oppfylle den rettssikkerhetsstandard som det er redegjort for i kapittel 6.1.

Siden rettssikkerhet bygger på lov er det ikke tilstrekkelig at en metode *hevdes* å være sikker av andre grunner, for eksempel at politiet benytter en bestemt type velprøvd teknologi, eller fordi det stilles strenge kompetansekrav til de tjenestemenn som skal bruke metoden. Dette er gode tiltak, men slik jeg oppfatter EMDs uttalelser skal de primært være forankret i lovteksten.

Derfor er ikke *politiets egeninteresse i* å utføre en kvalitativt god etterforsking i seg å anse som en rettssikkerhetsgaranti. Metodekontrollutvalget har likevel vist til at nettopp denne egeninteressen vil nøytralisere risikoen for at uvedkommende bruker politiets trojaner til å skaffe seg tilgang til mistenktes datasystem. Ifølge Metodekontrollutvalget innebærer det at risikoen " til en viss grad vil regulere seg selv", og (samme sted) at ved

"politiets installasjon av programvare for å muliggjøre dataavlesing kan slike svakheter utnyttes. Det innebærer at også andre kan utnytte de samme svakhetene. I tillegg vil politiets programvare kunne inneholde svakheter som kan utnyttes av andre. … Det er for utvalget opplyst at selv kriminelle som foretar innbrudd i datasystem regelmessig tetter de sikkerhetshull som er utnyttet, for å verne om det datasystemet de har skaffet seg kontroll over. Det samme vil selvsagt også politiet kunne gjøre."[45]

Jeg tror denne tilnærmingen er utilstrekkelig i forhold til å skape sikkerhet mot misbruk av trojaneren. Utvalget skiller ikke klart mellom sårbarhet som politiet selv skaper og må ta ansvaret for og sårbarhet som allerede eksisterer på systemet. Utvalget er til dels inne på mellomformer som

[45] NOU 2009: 15 s. 248.

beskrevet i kapittel 3.4. Så det blir uklart hvor langt man mener at politiets ansvar strekker seg. Da er det behov for at lovteksten er tydelig.

Problemstillingen er ny fordi de øvrige politimetodene ikke har medført noen vedvarende *datasårbarhet* for mistenkte. Det grunnleggende spørsmålet er om det i det hele tatt *er mulig* å anvende polititrojaner i politimetoder uten risiko for misbruk av tredjeperson.

Spørsmålet kan bare besvares på grunnlag av en teknisk utredning av et kompetent uavhengig organ som redegjør for risikoen ved installering av trojaneren og om risikoen kan kontrolleres. Med kontroll menes at trojaneren i konkrete tilfelle kan skjermes slik at den er til eksklusiv bruk for kompetent myndighet. En slik utredning er ikke innhentet av Metodekontrollutvalget og lovgivers beslutningsgrunnlag er følgelig helt utilstrekkelig på dette viktige punkt, med mindre Justisdepartementet sørger for å innhente en slik utredning.[46]

Metodekontrollutvalget stiller imidlertid krav om at politiet opplyser

”hva slags programvare … som er benyttet…, herunder angivelse av leverandør, leverandørens programnavn og produktnavn, versjonsangivelse …”.[47]

Min innvending er at slike opplysninger gir informasjon om den teknologi som faktisk er benyttet av norsk politi, men er utilstrekkelig i forhold til å håndtere *risikoen* som er beskrevet.

Sett at norsk politi bruker en trojaner som er utviklet av Federal Bureau of Investigation (FBI) eller National Security Agency (NSA) i USA, eller av fransk etterretningstjeneste, og pliktoppfyllende opplyser om dette i politirapporten. Eller at politiet opplyser å ha brukt teknologi fra en kommersiell aktør, og man vet at denne aktøren har store leveranser til utenlandske statlige overvåkingsprosjekter. Det er slike opplysninger Metodekontrollutvalget mener at bør gis i politirapporten. Men gir opplysningene grunn til å føle seg betrygget? Og kan den etterhåndskontroll som utvalget derved legger opp til anses tilstrekkelig i forhold til risikoens karakter? Burde ikke lovgiver ta stilling til hvilken teknologi som kan anvendes *i forkant av innføring av metoden?* Refleksjoner av denne art er helt fraværende i Metodekontrollutvalgets utredning.

På denne bakgrunn synes loven å burde oppstille krav om at dataavlesing bare kan skje ved bruk av nasjonal teknologi, som forbeholdes for nasjonalt politi, og ikke kan deles internasjonalt med lignende tjenester. Videre bør teknologien skiftes ut med jevne mellomrom for å sikre seg mot risiko som følge av teknologilekkasje. Dersom teknologien holdes hemmelig er den også mindre søkbar, og dermed har man i hvert fall prøvd å skjerme sårbarheten.

Til sist, hva med den danske lovbestemmelsen og andre land som har innført dataavlesing som selvstendig metode; kan de opprettholde metoden uten å dokumentere at ovennevnte rettssikkerhetsgarantier er ivaretatt? Eller må metoden i så fall inntil videre suspenderes?

I henhold til denne analysen *må metoden suspenderes* dersom den er innført uten at dette rettssikkerhetsspørsmålet er håndtert. Begrunnelsen er at *selve innføringen av lovhjemmelen* er et inngrep i rettighetene etter EMK art. 8.1, og den må da oppfylle vilkårene i bestemmelsens annen del. Dette gjelder uavhengig av om metoden rent faktisk benyttes eller ei. Dersom rettssikkerhetsvilkårene ikke er oppfylt foreligger en krenkelse av borgernes rettigheter etter EMK

[46] Se NOU 2009:15 kap. 23.1.3 om Metodekontrollutvalgets undersøkelser.

[47] NOU 2009: 15, s. 248.

art. 8, som enhver borger kan prøve. Det vises til Klass mot Tyskland (1978) pkt. 41, som er fulgt opp senere, se for eksempel AEIHRE pkt. 69, hvor dette premisset ble akseptert som sikkert av den innklagete stat (Bulgaria).

Det kan ikke utelukkes at situasjonen er som nevnt, både i Danmark og andre europeiske land. Hvis man har tenkt på samme måte som Metodekontrollutvalget, har man vært opptatt behovet for metodens og dens effektivitet, og i mindre grad av risikomomentene. Utvalget opplyser nemlig særlig å ha "fokusert på å kartlegge behovet for metoden og dens antatte effektivitet".[48]

Dersom man under lovforberedelsene ikke har spurt andre stater om noe har gått galt, har man neppe fått opplysning om det heller. Andre stater har kanskje *ikke evne til å oppdage misbruk*, siden dette er noe som nødvendigvis skjer skjult. Det er heller ikke noe som mistenkte lett oppdager. Dersom metoden innføres under henvisning til at andre stater har innført den, *kan det skje en gjensidig legitimering* av metoden, uten at noen utreder eller beslutningstaker noensinne har stilt grunnleggende kritiske spørsmål om risikoen. Da er borgernes rettssikkerhet i fare.

Lover

Ekomloven	Lov om elektronisk kommunikasjon av 4. juli 2003 nr. 83. (Norge)
Norsk straffelov 1902	Almindelig borgerlig straffelov av 22. mai 1902 nr. 10 (straffeloven). (Norge)
Retsplejeloven	Lov om rettens pleje, LBK nr. 1237 af 26.10.2010. (Danmark)
Straffeprosessloven	Straffeprosessloven (lov nr. 25/81). (Norge)

Forkortelser: Organisasjoner

ACPO	Association of Chief of Police Officers (UK)
ENFSI	European Network of Forensic Science Institutes
SWGDE	Scientific Working Group on Digital Evidence (USA)

Litteratur

Casey (2004)	Eoghan Casey *Digital Evidence and Computer Crime* San Diego, CA, USA, 2004.
Carrier (2010)	Brian Carrier *File System Forensic Analysis* Boston, MA, USA, 2005. 9th printing 2010.
Gomard (2008)	Bernhard Gomard m.fl. (red.) *Kommenteret retsplejelov* 8. utg., København, 2008.

[48] NOU 2009 : s. 236.

Hernes (2010)	Helga Hernes *EOS-utvalgets kontroll av "de hemmelige tjenester"* Dag Wiese Schartum (red.). Overvåking i en rettsstat. Fagbokforlaget 2010. Kapittel 16.
Høgberg/Kinander (2011)	Alf Petter Høgberg og Morten Kinander *Det formelle legalitetsprinsippet og rettskildelæren* TfR 1/2011 s. 15-55.
Smith (2011)	Eva Smith m.fl. *Straffeprosessen* 2. utg. København, 2011.
Stub Stub (2011)	Marius Stub *Tilsynsforvaltningens kontrollvirksomhet* Phd.-avhandling nr. 41, juridisk fakultet, Universitetet i Oslo, 2011.
Sunde (2006)	Inger Marie Sunde *Lov og rett i cyberspace* Bergen. 2006.
Sunde (2011)	Inger Marie Sunde *Automatisert inndragning* Complex 3/2011 Unipub AS. Oslo. (Phd-avhandling nr. 37, juridisk fakultet, UiO, 2010).
Toftegaard Nielsen (2010)	Gorm Toftegaard Nielsen *Dataflæsning*. Dag Wiese Schartum (red.). Overvåking i en rettsstat. Fagbokforlaget 2010. Kapittel 9.

Offentlige utredninger m.v.

Ds 2005: 6	Brott och brottsutredningi IT-miljö (Sverige)
Ju 2008:01	Polismetodutredningen (Sverige)
NOU 1997: 15	Etterforskingsmetoder for bekjempelse av kriminalitet (Politimetodeutvalget). (Norge)
NOU 2003: 27	Lovtiltak mot datakriminalitet – delutredning I (Datakrimutvalget) (Norge)
NOU 2007: 2	Lovtiltak mot datakriminalitet – delutredning II (Datakrimutvalget) (Norge)
NOU 2009: 15	Skjult informasjon – Åpen kontroll (Metodekontrollutvalget) (Norge)
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)
SOU 2005: 38	Tillgång till elektronisk kommunikation i brottsutredningar m.m. (Sverige)
SOU 2009: 1	En mer rätssäker inhämntning av elektronisk kommunikation i brottsbekämpningen. (Sverige).
SOU 2010: 103	Särskilda spaningsmetoder (slutbetänkande) (Sverige).

Netthenvisninger

Om keystroke logging:	http://en.wikipedia.org/wiki/Keylogging (besøkt 12.11.2010).
Om EMSEC og Tempest	http://encyclopedia2.thefreedictionary.com/TEMPEST (besøkt 12.11.2010).