DET NASJONALE STATSADVOKATEMBETET

FOR BEKJEMPELSE AV ORGANISERT OG ANNEN ALVORLIG KRIMINALITET

Samferdselsdepartementet
Postboks 8010 Dep
0030 Oslo

Deres referanse	*Vår referanse*	*Dato*
	13/10-3	9. april 2010

HØRING OM DATALAGRING

1. Innledning

Det vises til Justisdepartementets brev av 16. mars 2010 hvor høringsfristen er satt til 12. april 2010.

På bakgrunn av den offentlige debatt som har vært rundt spørsmålet om direktivet i det hele tatt skal implementeres i Norge, vil Det nasjonale statsadvokatembetet (NAST) i punktene 1 til 5 drøfte mer generelle spørsmål, særlig om det sterke behov politi og påtalemyndighet har for at direktivet blir gjennomført i Norge.

En vil deretter i punkt 6 gå mer inn på konkrete spørsmål rundt lovforslaget.
I høringsuttalelsen vil NAST bruke betegnelsen trafikkdata som en fellesbetegnelse på trafikk, lokalisering og identifikasjonsdata.

1.1 Generelle kommentarer

Begrunnelsen for direktivet er å sikre politi og påtalemyndighet i Europa et helt nødvendig verktøy for å avdekke, etterforske og rettsforfølge alvorlig kriminalitet. Særlig terror og annen organisert kriminalitet.

Utarbeidelsen av direktivet er basert på de erfaringer europeisk politi og påtalemyndighet har hatt gjennom mange år ved bruk av teledata. Politi og påtalemyndighet i de forskjellige land har gjort den samme erfaring; disse data er helt sentrale, nødvendige og viktige bevismidler.

Det nasjonale statsadvokatembetet vil derfor innledningsvis slå fast -

datalagringsdirektivet er avgjørende for fremover å kunne motvirke organisert kriminalitet og terror på en effektiv måte.

Det er ikke mulig å være for en effektiv bekjempelse av terror og organisert kriminalitet (selv kun med moderate virkemidler) og samtidig være mot gjennomføringen av datalagringsdirektivet. Å være for bekjempelse av organisert kriminalitet og samtidig mot implementering av datalagringsdirektivet er i realiteten en selvmotsigelse. Å ikke gjennomføre datalagringsdirektivet vil innebære en merkbar reell nedprioritering av kampen mot organisert og annen alvorlig kriminalitet.

Postadresse:	**Kontoradresse:**	**Telefon:**	**Telefax:**
Postboks 8044 Dep 0030 OSLO	Brynsalléen 4 0667 OSLO	23 17 42 00	23 17 42 10

Videre påpekes det at å avverge, redusere og oppklare organisert og annen alvorlig kriminalitet ikke er politiets ansvar alene. I en rettsstat må alle borgere, institusjoner og organer bidra idet bekjempelse av organisert kriminalitet og terror er en forutsetning for at en rettsstat skal fungere.

Politiets behov kontra borgernes personvern er derfor en for snever problemstilling. Borgernes berettigede vern mot alvorlig kriminalitet og beskyttelse av sentrale samfunnsfunksjoner kommer her også inn med tyngde.

Det nasjonale statsadvokatembetet er imidlertid ikke imot at en innfører ytterligere rettssikkerhetsgarantier opp mot bruken av trafikkdata så lenge garantiene ikke gjør den praktiske bruken av dataene unødig tungvint.

Det nasjonale statsadvokatembetet støtter i det store og hele de forslag høringsbrevet fremmer, men har innvendinger mot forslaget om krav til skjellig grunn til mistanke mot konkret person jf nedenfor under punkt 6.1. Det er videre et klart behov for hastekompetanse jf punkt 6.6 nedenfor.

1.2 Politiets lange erfaring med bruk av trafikkdata

I Norge har politi og påtalemyndighet brukt trafikkdata for mobiltelefoner i over 16 år. Det var for eksempel en viktig del av bevisbildet allerede i "Skriksaken" i 1994.

Implementeringen av direktivet medfører derfor ikke en stor og fundamental endring i forhold til dagens situasjon slik en rekke aktører i debatten har hevdet.

Det er forventet at teleselskapene vil slutte med frivillig lagring av teledata i en ganske nær fremtid. Enkelte teleselskaper skal visstnok allerede ha startet med å la være å registrere slike data.

Hvis man da ikke har en lov som pålegger lagring vil *den endrede situasjon* bestå i at norsk politi settes i en situasjon vi aldri tidligere har vært. Det er et faktum at så lenge de kriminelle har hatt mobiltelefon har politiet hatt tilgang på trafikkdata. Ingen har noen gang brukt mobil eller internett i Norge uten at politiet har hatt tilgang på deres trafikkdata.

Det er i denne sammenheng viktig å påpeke at innføringen av moderne teknologi som internett og mobiltelefon har effektivisert og gitt kriminelle muligheter de ikke hadde tidligere. Denne effektiviteten har vært balansert av rettsstatens muligheter til å følge elektroniske spor.

Narkotikatrafikken blir fleksibel og hurtig når leverandør kurer og mottaker ikke må avtale overleveringssted ved kurerens avreise, men fleksibelt kan avtale og endre dette underveis. Det veies opp av at de etterlater elektroniske spor.

Den som tidligere skulle få tak i barnepornografi måtte enten få dette overlevert fysisk eller få det adressert til seg per post, begge deler medførete en ikke ubetydelig oppdagelsesrisiko. I dag er materialet bare ett museklikk unna på internett, til gjengjeld legges det igjen en digital adresse som lagres.

Hvis Norge velger å ikke innføre direktivet vil vi få en situasjon hvor de kriminelle har alle fordelene moderne teknologi gir. Konsekvensene av dette er uoversiktelige, en kan driste seg til å mene at konsekvensene av dette eventuelt burde utredes før en opplyst beslutning kan fattes. Så vidt vites er det ingen samfunn noen gang som har hatt en situasjon hvor ikke historiske spor fra mobil og internettbruk er sporbare.

Det er videre verdt å merke seg at det ikke har fremkommet noe større antall saker med personer som mener personvernet er overtrådt i forbindelse med politiets bruk av trafikkdata. Tatt i betraktning at dette har pågått i over 16 år, er det lave antallet oppsiktsvekkende og en indikator på at faren for misbruk av trafikkdata i forbindelse med innføring av direktivet er overdrevet av en del motstandere av direktivet.

1.3 Politiets behov

For politiet krever det mye ressurser å innhente og bearbeide trafikkdata. Det gjøres likevel, fordi nytten klart overstiger kostnaden.

I dag innhentes trafikkdata i ca 50% av de alvorlige straffesakene jf Kripos undersøkelse. I de alvorligste (av de alvorlige) sakene er prosenten langt høyere. Det nasjonale statsadvokatembetet som er overordnet påtalemyndighet for Kripos og PST har siden opprettelsen i 2005 ikke hatt noen sak vedrørende organisert kriminalitet eller terrorbestemmelsene hvor ikke trafikkdata har utgjort eller utgjør en viktig del av bevisbildet. Særlig i de store etterforskingsprosjektene mot organisert kriminalitet har trafikkdata hatt stor betydning.

Slike data gir vital informasjon om bevegelser og kontaktmønstre tilbake i tid. Dette er ikke minst viktig når en skal bevise kriminelle organisasjoners hierarki, omfang, ordrelinjer osv. Dette er igjen for eksempel sentralt opp mot anvendelsen av straffeloven § 60a.

Trafikkdata er objektive bevismidler som er viktige for rettssikkerheten

En klar fordel med trafikkdata er at de er objektive. De er ikke som vitneforklaringer påvirket av inntrykk, hukommelse osv.

Moderne politiarbeid hviler ikke på én politimetode eller bevistype alene. Det er summen av de forskjellige metoder og bevis som er viktig.
De forskjellige metodene utfyller hverandre, tetter hull og opplyser saken.

Kan også frifinne

For dårlig opplysning av faktum kan medføre at politiet griper feil og vi risikerer at uskyldige blir siktet og i spesielle tilfeller domfelt. Trafikkdata motvirker dette.

Uskyldige som kommer i politiets søkelys i en etterforsking kan bli sjekket ut av saken fordi trafikkdata viser at deres forklaring om at de hadde alibi for gjerningstidspunktet med all sannsynlighet er riktig.

Ved fastsetting av for eksempel drapstidspunkt vil innhenting av data fra offerets mobiltelefon være et viktig bidrag. I den andre Fritz Moen saken var et av de avgjørende spørsmålene om avdøde ble drept natt til lørdag (siste sikre observasjon hvor Fritz Moen hadde alibi) eller minst et døgn senere. I dag ville trafikkdata fra avdødes mobil kunne gitt viktige bevis rundt dette.

Trafikkdata er videre sentrale ved tidfesting og rekonstruering av hendelsesforløp. Noe som er sentralt i nesten alle større etterforskinger.

I sin store betydning for å opplyse saken er dataene også viktige for rettssikkerheten.

Også i de sakene hvor dataene *ikke føres* som bevis, er de viktige fordi de opplyser et faktum som forklaringer avgitt i saken kan avstemmes mot. Dataene gir følgelig mindre spillerom for uriktige forklaringer, noe som ikke alltid synliggjøres i bevisførselen. Det er derfor sannsynlig at

nytteeffekten er større enn den som Metodekontrollutvalget har målt, selv om utvalget legger til grunn at nytten er større under etterforskingen enn iretteføringen (NOU 2009: 15 s.117).

Det er en gjenganger i embetets saker at de tiltalte i sine forklaringer nekter for inkriminerende kontakter, bekjentskaper og bevegelser i tingretten. Dette blir så motbevist ved trafikkdata-analyser presentert under tingrettsbehandlingen. I lagmannsretten har de tiltalte lært leksen sin og tilpasser sin forklaring til trafikkdataene. I slike situasjoner vil trafikkdataene spille en langt mindre rolle under bevisførselen i lagmannsretten fordi det ikke er uenighet mellom partene. Typisk vil de også i liten grad bli omtalt i dommen, men de har likevel hatt stor betydning og levert en helt sentral premiss for resultatet.

Bare vissheten om at det finnes trafikkdata gjør at siktede i straffesaker ofte allerede under etterforskingen nødig vil forklare seg uriktig om bekjentskaper og kontakter.

Organisert kriminalitet og terror

Trafikkdata er som nevnt bevismessig av stor betydning i saker mot organisert kriminalitet.
I organisert kriminalitet/terror holder ledere avstand til det utøvende element. De gir beskjeder og ordre, ofte over store avstander og er avhengig av telefon eller epost. Trafikkdata bakover i tid som viser kontaktnett og mønstre vil kunne være avgjørende.
Det er i praksis umulig å rulle opp en kriminell organisasjon uten bruk av trafikkdata. I flere saker danner den periode det er mulig å innhente trafikkdata rammene for saken.

Det nasjonale statsadvokatembetet og Kripos er nå i avslutningsfasen av iretteføringen av Norgeshistoriens største narkotikasak (Op Broken Lorry). Totalt er 35 personer rettskraftig domfelt og det er idømt 289 rettskraftige fengselsår. To av lederne ble i 2009 de første i Norge som ble idømt 21 års fengsel for narkotikaforbrytelser. Ytterligere to ville fått 21 år hvis de ikke hadde erkjent og fått strafferabatt. I denne saken har teledata fra Norge og Nederland vært av avgjørende betydning. Flere av de sentrale aktørene hadde sannsynligvis ikke blitt domfelt hvis en ikke hadde trafikkdata. Uten trafikkdata hadde tiltalene også blitt langt mindre omfattende. For eksempel når en av kurerene i saken, fører av et vogntog, ble pågrepet med narkotika, gikk politiet inn på hans telefon, og kunne se hvilke telefoner han hadde ringt. Kripos gikk deretter inn på trafikkdataene til disse telefonene bakover i tid og kunne se når sjåføren og de andre kontaktene hadde vært på et konkret sted. Denne sporingen gjorde at vi fikk dømt en rekke personer for innførsler i inntil 5 måneder tilbake i tid. Fem måneder er som kjent maksimallagringstiden i Norge. Det er nærliggende å tro at flere innførsler og personer ville ha blitt avdekket hvis trafikkdataene gikk enda lenger tilbake enn bare 5 måneder.

I en meget alvorlig narkotikasak som ble aktorert av embetet for Oslo tingrett i februar/mars i år, var historiske trafikkdata fra Sverige avgjørende for skyldspørsmålet for 2 av de fire tiltalte. Basestasjonsutskriftene viste at de 2 tiltalte i strid med deres egne forklaringer reiste sammen med hovedmannen i saken fra Østfold via Uddevalla, Malmø og Jønkøping hvor de møtte kureren som fraktet heroinen til Sverige. De tre impliserte fra Norge og kureren reiste deretter sammen til Norrkøping. Neste dag reiste hovedmannen og en av de andre impliserte videre mot Norge med narkotikaen. Vi snakker om et reisemønster som gikk over tre dager. Trafikkdata og særlig basestasjonsregistreringene var avgjørende for å bevise at de tre reiste samtidig fra Østfold, beveget seg parallelt og ankom Norrkøping samtidig. Trafikkdata og basestasjonsutskrifter var senere avgjørende for å påvise at de tre fra Østfold på et senere tidspunkt reiste sammen for å sikre kurerbilen.
De to som nektet straffeskyld ble i tingretten dømt til fengsel i henholdsvis 12 og et halvt og åtte års fengsel. Dommen er ikke rettskraftig.

Personer som hevder at politiet ikke har et behov eller at bevisbetydningen er overdrevet, kan neppe ha fulgt slike saker i retten.

I saker knyttet til *terrorbestemmelsene* som ved organisert kriminalitet, er teledata av stor betydning for å bevise kontaktmønstre, bekjentskaper og bevegelser.

Internasjonalt politi- og påtale samarbeid
Allerede i dag lider norsk politi i internasjonal sammenheng i forhold til bl.a. Datatilsynets sletteregel på 3 uker for internettrafikk. Dette problemet har dukket opp en rekke ganger ved større internasjonale aksjoner og rettsanmodninger fra enkeltland i saker om seksuelle overgrep og bilder mot barn på Internet.

Hvis ikke Norge gjennomfører direktivet vil det åpenbart også kunne skade oss i andre type saker og vi risikerer at utenlandsk politi i praksis vil bli mindre interessert i gjøre det lille ekstra som er nødvendig for et vellykket resultat, fordi vi ikke kan hjelpe dem med en gang noe så elementært og viktig som trafikkdata. Internasjonalt politi- og påtalesamarbeid er basert på gjensidighet hvor man høster det man sår.

Det nasjonale statsadvokatembetet og Kripos mottar en svært stor andel av alle rettsanmodninger andre land sender til Norge. Blant de aller vanligst forespørslene vi får fra utlandet er søk etter trafikkdata i Norsk nett. Motsatt er en av de vanligste anmodningene vi sender til utlandet begjæringer om søk etter trafikkdata i deres nett. Dette samarbeidet er av vesentlig betydning for å bekjempe den internasjonale organiserte kriminaliteten. Det vil være oppsiktsvekkende hvis Norge som eneste land i vår region ikke lenger vil kunne bidra med denne type informasjon.

Manglende implementering kan føre til at Norge anses som "fristed"
Hvis Norge i motsetning til de øvrige europeiske land, ikke gjennomfører direktivet, vil det være en klar fare for at organiserte kriminelle og terrorister i enda større grad enn i dag trekkes mot Norge. Norge vil kunne bli ansett som en tilnærmet "safe haven" på grunn av klart dårligere metodemuligheter enn ellers i Europa.

Forenlig med EMK art. 8
Det nasjonale statsadvokatembetet er enig med departementene i at direktivet er forenlig med de krav som stilles i EMK art. 8.

Vi mener videre at kriminalitetssituasjonen med utstrakte kommunikasjonsmuligheter og forflytning over landegrensene gjør at det burde være *et aktuelt politisk spørsmål å innføre datalagring uavhengig av direktivet* for å sikre muligheten for bekjempelse av organisert og annen alvorlig kriminalitet.

Ifølge høringsnotatet gjelder inngrepet personvernet til de alminnelige brukerne av elektroniske kommunikasjonstjenester. Etter NASTs mening er dette en for snever tilnærming, fordi personvernspørsmålet i høy grad også gjelder kriminalitetsofrenes vern mot krenkelser av sin integritet og eiendom. Spørsmålet om lagringsplikt har uansett en omkostning for personvernet. Hvis datalagring *ikke* innføres er det personvernhensyn og fundamentale rettigheter til en mengde kriminalitetsofre som myndighetene velger å se bort fra. I tillegg til personverninteressene kommer samfunnsinteressen (alle borgernes interesse) i at alvorlig kriminalitet som svekker samfunnsinstitusjonene (alvorlig organisert kriminalitet, terror, korrupsjon, motarbeidelse av rettsvesenet m.v.) oppklares.

2. Nærmere om politiets bruk av data

2.1 Tilgangen på alternative metoder

Enkelte av de personer/organer som *ikke* arbeider med alvorlig kriminalitet og bruk av trafikkdata har hevdet at politiets behov er dekket ved hjelp av *"frysbestemmelsen" i strpl. § 215a* og at en derfor ikke behøver noen innføring av datalagringsdirektivet.

Til det er å si at "frysbestemmelsen" har kun virkning fremover i tid. Den er derfor helt ubrukelig med tanke på å skaffe trafikkdata av betydning i saker hvor den straffbare handling er begått; for eksempel et ran av NOKAS typen, drap med ukjent gjerningsmann eller en terrorhandling.

Bestemmelsen er videre ubrukelig med tanke på å vise kontaktmønstre og bevegelser bakover i tid for eksempel i saker om organisert kriminalitet.

Det er videre slik at behovet for trafikkdata knyttet til et nummer ofte viser seg etter lengre etterforsking. Typisk fordi de siktede bruker flere telefonnummer og ønsker å holde i hvert fall enkelte av disse "hemmelig". Når politiet innhenter data for disse er brukerne allerede pågrepet. Frysbestemmelsen som virker fremover i tid vil i slike situasjoner være meningsløs.

Kort fortalt er "frysbestemmelsen" ubrukelig med tanke på å erstatte den bruk politi- og påtalemyndighet i dag har av *historiske trafikkdata.*

NAST mener at spørsmålet om datalagring er nødvendig, må settes inn i en kontekst hvor det er vesentlig å merke seg at dataene gir grunnlag for å avdekke *hvem* som kan være implisert i straffbar virksomhet, og at det *ikke finnes alternative metoder* som er mindre inngripende for å oppnå det samme.

Ofte er situasjonen at det ikke finnes alternative metoder overhodet for politiet til å gå tilbake i tid. Nesten alle metoder har som forutsetning at de virker fremover i tid fra politiet setter i gang for eksempel kommunikasjonskontroll. Den kan selvfølgelig ikke foretas bakover i tid. Den kan ikke vise om to telefoner hadde hyppig daglig kontakt forut for at politiet startet sin etterforsking.

I tillegg til det som er angitt ovenfor utnytter politiet trafikkdataene bl.a. på følgende måte:

Trinn 1: Utgangspunktet er at politiet har en kommunikasjonsadresse. For aktivitet på nettet er dette en IP-adresse + et tidspunkt (dynamisk IP-adresse). For annen aktivitet er det hovedsakelig tale om mobiltelefonnumre. På grunnlag av kommunikasjonsadressene kan politiet få rede på *identiteten* til sluttbrukeren. Identiteten kan fremgå av offentlige registre (telefonkatalogen) eller kan innhentes fra tilbyder ("ISP"). For aktivitet på nettet må den alltid innhentes fra ISPen, fordi de offentlige registrene ("whois") ikke viser hvem som til enhver tid disponerer IP-adressen, den er allokert til ISPen selv.

Trinn 2: Dersom politiet får opplyst sluttbrukerdataene (identitet) har man et utgangspunkt for videre etterforsking. Det kan for eksempel gå ut på innhenting av trafikkdata knyttet til den aktuelle kommunikasjonsadressen. Ved organisert kriminalitet kan trafikkdataene kaste lys over lovbryterens kontaktnett. Det kan bidra til å avdekke identiteten til andre impliserte (trinn 1) og muligens til å innhente trafikkdata på dem også (trinn 2).

Hva som skjer i trinn 2 beror selvsagt på sakens karakter. Andre etterforskingsskritt enn de som er nevnt kan være aktuelle. I internettsammenheng er det ikke mulig å få ut trafikkdata som kaster

lys over lovbryterens aktiviteter på nettet over en tidsperiode. For å gå videre må politiet vurdere bruk av ransaking og avhør av siktede. Vitnebevis med observasjoner om hva som foregikk på nettet, er ikke tilgjengelige, så bevis må hentes fra lovbryterens datamaskin. For å nå frem til datamaskinen må politiet ha opplysning om identitet og adresse. Dersom tilbyder ikke lagrer opplysninger som gir oversikt over hvilke sluttbrukere som bruker IP-adressene til forskjellige tider, er det ikke mulig å avdekke identiteten til lovbrytere på nettet, annet enn ved infiltrasjon, noe som er et utilstrekkelig alternativ, se nedenfor.

Internett:
Datalagring er *uomgjengelig nødvendig* for å avdekke identiteten til lovbrytere på internett. Siden IP-adressene ikke tilhører bestemte sluttbrukere (slik telefonnumre gjør), kan man ikke på grunnlag av en IP-adresse som er registrert én gang innlede etterforsking fordi den samme IP-adressen er involvert i en straffbar handling på et senere tidspunkt. Det er kort og godt ikke "samme nummer" som er benyttet (i betydningen tilhørende samme sluttbruker). For at ISPen skal kunne gi opplysninger om sluttbruker, må tidspunktet for internettaksess registreres. Det er ensbetydende med at ISPen må holde oversikt over hvem som til enhver tid disponerer IP-adresser. Således må datalagringen omfatte alle brukerne.

Iblant kan politiet bruke infiltrasjon. Metoden er bare anvendelig i sann tid og er mer inngripende overfor den annen part enn å be om sluttbrukerdata på en person. Infiltrasjon har også bare begrenset nytteeffekt for å oppklare forhold som alt er begått. De fleste saker starter med tips eller anmeldelse. Dersom tilbyder ikke har sluttbrukerdata knyttet til IP-adressene for en periode tilbake i tid, har ikke politiet noe grunnlag for målrettet etterforsking mot dem det gjelder. På internettsiden finnes det altså ikke noen annen mindre inngripende metode for å avdekke identiteten til lovbrytere, enn å rette en forespørsel til tilbyder. Bestemmelsen om sikringspålegg, jf. strpl. § 215 a er ikke et dekkende alternativ, fordi den som nevnt bare gir hjemmel for å sikre data som alt er lagret. Dersom tilbyder lojalt og profesjonelt har fulgt ekomloven § 2-7 annet ledd, er dataene slettet så det er ingen data å sikre. Derfor er lagring nødvendig.

Mobiltelefoni:
På mobiltelefonisiden skulle man kanskje tro at bevistilbudet var mer sammensatt, fordi det er tale om lovbrudd i "den fysiske verden" hvor det blant annet kan finnes vitner til det som skjer. Typiske lovbrudd er narkotikaovertredelser, grove ran og torpedovirksomhet, men det kan også være "hvitsnippkriminalitet" som innsidehandel og kursmanipulasjon. Erfaring gjennom mer enn 16 år viser imidlertid at kommunikasjonsdataene har stor betydning i bevistilbudet jf ovenfor.

Dette er for øvrig noe enhver som har fulgt med i alvorlige straffesaker i Norge i samme periode kan bekrefte. Kontaktmønstre og bevegelser ut fra basestasjonsregistreringer har vært viktige i en rekke saker.

Kommunikasjonsavlytting har utvilsomt verdi, men ikke alene. For å vite hvem dette skal rettes mot, må et grunnlag være etablert. Dette grunnlaget skapes av en trafikkdataanalyse. Kommunikasjonsavlytting er særdeles inngripende og må rettes mot korrekt adressat. Produksjon av et forutgående informasjonsgrunnlag basert på analyse av trafikk- og lokaliseringsdata er derfor nødvendig. Kommunikasjonsavlytting fremover i tid kan imidlertid ikke nødvendigvis oppklare forhold som ligger tilbake i tid. Kommunikasjonsavlytting er mer inngripende enn en teledataanalyse, og har et mer begrenset bruksområde. NAST kan ikke se at det står andre og mindre inngripende metoder til rådighet i slike saker enn analyse av trafikkdata. Datalagring sikrer at tilbyder ikke systematisk sletter disse dataene.

2.2 Et regelverk i ubalanse

Dersom ikke lagring gjennomføres, samtidig som slettingsplikt/lagringsforbud opprettholdes, må det reises spørsmål ved lovverkets sammenheng mellom kriminalisering og muligheten for å stille lovbrytere til ansvar. Myndighetene (Regjering og Storting) har ansvar for – gjennom et balansert lovverk – å sikre mulighet for effektiv rettshåndhevelse.

EMD har understreket at eksistensen av straffebud på papiret ikke er tilstrekkelig for å verne om retten til privat liv og privat integritet. I *K.U mot Finland (2008)* uttalte EMD at "...the existence of an offence has limited deterrent effects if there is no means to identify the actual offender and bring him to justice" (pkt. 46). EMD krevde i tillegg at det tilrettelegges for "effective investigation and prosecution" (pkt. 46). Dette er i samsvar med det syn som EMD la til grunn i *M.C. mot Bulgaria (2003)* som gjaldt myndighetenes plikt til å besørge adekvate forhold for å etterforske og oppklare voldtekt. Tilsvarende syn er kommet til uttrykk i *Osman mot Storbritannia (1998),* som gjaldt plikten til å avverge krenkelse mot liv.

Spredning og nedlasting av overgrepsbilder skjer hovedsakelig ved bruk av Internett. Som vist tidligere er trafikkdata koblet med IP-adresse nødvendig for å oppspore gjerningspersoner (med mindre det også finnes kredittkortopplysninger). Mye av virksomheten skjer imidlertid utenom betalingsbelagte tjenester, særlig på fildeling. Tjenesten innbyr ikke til at etterforskeren innleder en samtale om utvekslingen, fordi deltakerne deler materialet anonymt direkte fra sine maskiner. Infiltrasjon på fildelingstjenester er derfor ikke en aktuell alternativ metode.

NAST antar at sletteplikten for opplysninger med avgjørende betydning for oppsporing av lovbrytere på markedet for overgrepsbilder, jf. ekomloven § 2-7 annet ledd, neppe er forenlig med Norges internasjonale forpliktelser. Overgrepsbildene dokumenterer seksuelle overgrep, og avbildningen representerer en alvorlig krenkelse (overgrep) mot barnas personvern.[1] De internasjonale forpliktelsene krever ikke bare kriminalisering, men også at strafforfølgningen skjer effektivt og har allmennpreventiv virkning.

Her kan nevnes at Norge i oktober 2007 undertegnet Europarådets konvensjon om beskyttelse av barn mot seksuell utnytting og seksuelt misbruk. Konvensjonen stiller blant annet krav til etterforsking, straffeforfølging og til prosessuelle regler i saker som gjelder seksuell utnytting og misbruk av barn. Det vises også til FN's barnekonvensjon.

Dersom dataene slettes må man spørre seg om det er meningsfylt ressursbruk å prioritere arbeidet mot overgrepsbilder på nettet. Det samme gjelder "grooming", jf. strl. § 201 a. I realiteten gjelder det *all* nettbasert kriminalitet, som datainnbrudd, databedragerier og hvitvasking. Politiet er avhengig av at opplysninger om hvilke kommunikasjonsadresser som har vært brukt til forskjellige tidspunkt, er blitt lagret av tilbyder. I en rettsstat har myndighetene også et ansvar for å trygge ofrenes stilling, hvor det å stille lovbryteren til ansvar for sine handlinger er et sentralt element.

EMD har uttrykkelig avvist at en kompensasjonsordning fra tredjemann er et tilstrekkelig alternativ for strafforfølgning, jf. *K.U mot Finland (2008):*

[1] Se EUs "Safer Internet Program", www.circamp.eu, som har en sterk anbefaling om å gå vekk fra uttrykket "barnepornografi". Norge v/Kripos leder et internasjonalt prosjekt under circamp, som går ut på tipshåndtering og filtrering av overgrepsbilder på nettet.

"it is plain that both the public interest and the protection of the interests of the victims of crimes committed against their physical or psychological well-being require the availability of a remedy enabling the actual offender to be identified and brought to justice" (pkt. 47).

Uttalelsen gjaldt ISPen tilbud om erstatning til fornærmede, fordi de strenge taushetsreglene avskar muligheten for å oppspore en lovbryter på Internett. På grunn av sletteplikten har det norske rettssystemet den samme mangel på rettshåndhevelsesevne som Finland ble dømt for. I lys av dette kan det lovfestede pålegget om sletting av de nødvendige data for å iverksette strafforfølgning, ses som en krenkelse av ofrenes legitime krav på vern.

Slettingen motvirker også samfunnsinteressen i oppklaring av alvorlig kriminalitet, som iblant kalles "offerløs" fordi den ikke blir anmeldt. Rettshåndhevelsen må derfor skje på grunnlag av tips og politiets innsanking av bevis fra andre kilder, og her står trafikkdataene helt sentralt. NAST minner om den aktive rolle Norge har spilt i utviklingen av internasjonale tiltak mot korrupsjon, hvitvasking og grenseoverskridende organisert kriminalitet. De argumenter som er beskrevet over gjør seg gjeldende også her. Det har lite for seg å kriminalisere om man plikter aktivt å slette opplysninger som er sentrale for strafforfølgningen.

Oppsummering
NAST mener at datalagring er et målrettet tiltak som på egnet måte sikrer at Norge oppfyller internasjonale og menneskerettslige forpliktelser til å ha en rimelig effektiv rettshåndhevelse overfor alvorlig kriminalitet.

Med den ordning som høringsnotatet legger opp til sørger myndighetene for lagring av dataene i en begrenset tidsperiode, med klare krav til behandling, sikring, innsyn, tilsyn og sletting. Den foreslåtte ordning *balanserer de kryssende hensyn* og sørger for at regelverket på klar og forutsigbar måte regulerer lagring og bruk av kommunikasjonsdataene. Dog med klart unntak for forslaget til krav om skjellig grunn til mistanke mot konkret/bestemt person og fravær av hastekompetanse for påtalemyndigheten.

I et travelt, mobilt, urbanisert og internasjonalisert samfunn nyter borgeren stor individuell frihet. Myndighetene – herunder Datatilsynet – er ikke bare den velstilte lovlydige borgers representant, men skal ivareta alle, også ofrene og deres personvern. For den jevne borger er lagringen av kommunikasjonsdataene på de vilkår som er foreslått, ikke følbart, og man kan til enhver tid få innsyn i hva som er lagret om en selv. Det lille individuelle inngrepet som lagringen innebærer, bør enhver kunne akseptere som et bidrag til en rimelig effektiv rettshåndhevelse i fellesskapets interesse.

3. Datalagring - en prinsipiell nyskaping?

Høringsnotatet pkt. 2.1, fremholder at datalagring er en "prinsipiell nyskapning" fordi "det innføres en plikt til å lagre data og ... dette skjer for å imøtekomme myndighetenes behov." NAST er uenig i at datalagring er en "prinsipiell nyskapning". Rent konkret var *sletteplikten* som ble innført med ekomloven § 2-7 i 2003, en nyskapning.

Før 2003 var trafikkdataene i stor grad uregulerte, og det var ikke klart etablert at de, eventuelt hvilke av dem, som var å anse som personopplysninger og følgelig omfattet av krav til formålsbestemthet og sletting. Også i høringsnotatet s. 27 nederst, gis det uttrykk for at lagringen "ikke [vil] gjelde informasjon som er direkte knyttet til folks personlige identitet". Bortsett fra abonnementsdata ("identifikasjonsdata") som i hovedsak er offentlig tilgjengelige, er det altså tale om lagring av såkalte "indirekte personopplysninger".

Lagringsplikten har velkjente paralleller i regelverk som tar sikte på å hindre hvitvasking og terrorfinansiering, samt i regler om regnskaps- og oppbevaringsplikt. Også disse reglene er vesentlig begrunnet i myndighetenes kontrollbehov. De omfatter hele befolkningen i den utstrekning man bruker tjenestene til bank- og finansnæringen, eller er regnskapspliktig. Hvitvaskingsreglene går vesentlig lenger enn datalagringsdirektivet, fordi det gjelder en plikt til å rapportere til politiet om mistenkelige transaksjoner, mens datalagring bare innebærer lagring for et begrenset tidsrom. Politiet må selv be om utlevering vedrørende bestemte kommunikasjonsadresser.

Selv om lagringsplikten bryter med personvernprinsippet om at opplysningene ikke skal brukes til andre formål enn det *opprinnelige* formålet med innsamlingen, er det ikke noe nytt fenomen i norsk rett, og kan vanskelig sies å være en "prinsipiell nyskapning".

4. En kjølende effekt?

I høringsnotatet s. 41 nevnes faren for at datalagring kan ha en kjølende effekt på ytringsfriheten. Dette fremstår som en udokumentert påstand og synes i Norge første gang å ha vært fremsatt i Personvernkommisjonens uttalelse om datalagring, inntatt som vedlegg 1 til NOU 2009: 1 *Individ og integritet.* Denne uttalelsen står for Personvernkommisjonens egen regning, og er ikke en uttalelse "på europeisk nivå" fra artikkel 29 gruppen, slik det er opplyst i høringsnotatet øverst s. 25 (nettadressen der viser til Personvernkommisjonens uttalelse).

I uttalelsen står det følgende (s. 222 i NOU 2009: 1):

"Verdien av lagring må nemlig også veies opp mot effekter på frimodighet. Dette gjelder selv om formelle friheter ikke berøres, og selv om de registrerte data kun skal være tilgjengelige for politiet under regulerte forhold. Allerede vissheten av at noen *kan* lete seg fra til dine kontakter og dine bevegelser, både i det virkelige rommet og på Internett, kan være nok til å hemme borgere i utøvelsen av sine friheter til å samles, til å ytre seg og til å søke opplysninger."

Lenger ned på samme side trekker Personvernkommisjonen også i tvil trafikkdataenes betydning for oppklaring av kriminalitet. Man kan spørre seg hva slags fakta som ligger til grunn for uttalelsene (den tyske undersøkelsen som er nevnt har vist seg ikke å kunne dokumentere påstanden). Disse såkalte fakta stemmer i hvert fall ikke med norsk politi sin lange erfaring med bruk av disse dataene. Datalagring har man hatt i europeiske land i mange år, i et naboland som Danmark siden 2001, med full gjennomføring av direktivet også på internettsiden siden 2006. *De facto* har det vært datalagring også i Norge, på telefonisiden så lenge telefonen har eksistert. Som nevnt flere ganger har norsk politi brukt mobiltelefondata som viktige bevismiddel i minst 16 år.

Påstanden om at dette har noen effekt på frimodigheten savner ethvert empirisk grunnlag og fremstår heller ikke som nærliggende eller rimelig sannsynlig. Det skal ikke lagres opplysninger om innhold, dvs. hva man har sagt, hvor man har surfet på Internett m.v.. og terskelen for politiets tilgang til opplysningene skal heves. Dersom Personvernkommisjonen tenker på risikoen forbundet med *tilbydernes* tilgang til dataene, så har den eksistert like lenge som man har tilbudt kommunikasjonstjenestene. Frimodigheten har likevel ikke kjølnet.

Det er langt mer sannsynlig at god utbygning av elektroniske kommunikasjonstjenester/-nett, stadig lavere kostnader ved bruk av tjenestene, og gode muligheter for anonymitet, har ledet til at frimodigheten har *økt.* Det er ikke holdepunkter for at datalagring påvirker dette.

Til jussen kan det bemerkes at læren om "chilling effect" knytter seg til EMK art. 10 om ytringsfrihet. Datalagring er ikke et inngrep i EMK art. 10 som det står i høringsnotatet øverst s. 42, i tilknytning til uttalelsen om kjølende effekt. Datalagring er et inngrep i retten til "respekt for sitt privat liv ... og sin korrespondanse", jf. EMK art. 8. Da er spørsmålet om inngrepet er av en slik karakter at det er en trussel mot demokratiet, noe NAST ikke kan se at det er, se ovenfor punkt 1.3 side 5 og punkt 5 nedenfor.

5. Datalagring er ikke overvåking

NAST kan ikke se at datalagring representerer overvåking i en rimelig betydning av ordet. Det får være en sak for seg at man innen personvernteorien bruker 'overvåking' om enhver innsamling og behandling av personopplysninger for et bestemt formål. I normal språkbruk virker dette kunstig. Overvåking leder en til å tro at det er noen som følger med ens bevegelser i nåtid. Ikke at man avsetter visse elektroniske spor som blir lagret midlertidig i en gitt tidsperiode og kanskje blir innhentet av politiet til bruk i en etterforsking etter konkret mistanke.

Etter EMDs praksis er imidlertid spørsmålet om inngrepet representerer en trussel ("menace") mot demokratiet. Da er spørsmålet om inngrepet er hemmelig og resulterer i informasjonsoverlegenhet hos politiet fordi opplysningene lagres hos politiet (og sikkerhetstjenesten). I tre kjente saker har EMD prøvet om såkalt strategisk overvåking var forenlig med EMK art. 8. Det er *Klass (1978)* (ikke krenkelse), *Weber (2006)* (ikke krenkelse) og *Liberty (2008)* (krenkelse). Disse sakene gjaldt hemmelig informasjonsinnsamling basert på telefonavlytting og filtrering av elektronisk kommunikasjon på grunnlag av nøkkelord mv., for å skaffe etterretningsinformasjon (smlg. den svenske "FRA-loven"). Underretning til borgerne ble gitt på et svært sent tidspunkt, når det ikke lenger var forbudet med fare for å forspille formålet, mange år etter at overvåkingen fant sted.

Ordningen med datalagring kan ikke sammenlignes med de nevnte sakene. Ved datalagring er også informasjon om kommunikasjonen til *ansatte i politiet* omfattet av ordningen, og dataene skal *ikke* lagres hos politiet. Det foreligger ikke noe element av informasjonsoverlegenhet ved lagringen, og borgeren har innsynsrett i de opplysninger som er lagret om vedkommende. Dermed representerer ikke datalagringen noen trussel mot demokratiet i henhold til kriteriene som følger av den nevnte rettspraksis. Informasjonsoverlegenheten inntrer først når politiet får tilgang til dataene, og da stiller informasjonsbehandlingen seg likt med de andre opplysningene som inngår i en straffesak. Forslaget representerer ikke noe nytt mht bruken av kommunikasjonsdataene og terskelen for politiets tilgang skjerpes i forhold til i dag.

6. Konkrete merknader til lovforslaget

6.1 Krav til mistanke mot konkret person

På side 48 tredje avsnitt i høringsbrevet uttales at;
"En konsekvens av lovforslaget på dette punktet, er at politiet ikke lenger vil kunne få tilgang til data der det ikke lar seg bevise at det foreligger skjellig grunn til mistanke som knytter seg til en bestemt person".

Det er noe uklart hva forslaget mener med skjellig grunn til mistanke om en bestemt person. Menes det her, at en må være mer enn 50 % sikker på at det er en eller flere ukjente personer som står bak, ser en ingen innvendinger. Kreves det imidlertid at en er mer enn 50% sikker på hvem den ukjente gjerningsmannen er, har Det nasjonale statsadvokatembetet klare innvendinger.

Fordi dette vil fjerne muligheten til generelle basestasjonsutskrifter i en innledende fase i saker som gjelder for eksempel drap med ukjent gjerningsmann, terroranslag og NOKAs lignende ran.

Ved terroranslag vil teledata med all sannsynlighet være ett av få spor politiet kan arbeide ut fra når man i ettertid skal jakte på gjerningsmenn. Det er i forbindelse med etterforskingen nødvendig at politiet kan innhente basestasjonsutskrifter fra de basestasjoner som dekker for eksempel et bombeområde og har mulighet til å sjekke ut de personene som slår inn i den aktuelle perioden (for eksempel fra bomben ble eller antas ble plassert og til den gikk av). Dette for å fange opp personer som for eksempel rekognoserer, plasserer bomben, utløser bomben eller bidrar på annen måte og vitner. Dette må gjøres på et helt innledende stadium i etterforskingen og politiet vil typisk ikke ha noen konkret mistenkt. I hvert fall ikke skjellig grunn til mistanke mot en konkret person.
De samme hensyn gjør seg gjeldende for åstedet eller funnstedet for lik i drapssaker med ukjent gjerningsmann.

Lovforslaget er derfor alt for innskrenkende når det nå foreslås at det må foreligge konkret skjellig grunn til mistanke mot en bestemt person.

Et slikt forslag er direkte ødeleggende for politiets mulighet til å oppklare de alvorligste forbrytelser. Høringsbrevets uttalelse om at "muligheten for å realisere formålet med lagringsplikten – å bekjempe alvorlig kriminalitet – blir noe forfeilet" er en sterk underdrivelse.

Det kan ikke være et vilkår at politiet har sannsynlig identitet på personen før begjæring om trafikkdata sendes, når det nettopp er det å avdekke identiteten som er det sentrale poeng ved begjæringen og etterforskningsskrittet.

Det er her nødvendig at man faller ned på en "alternativ to" lignende løsning, se høringsbrevet jf side 48 siste avsnitt hvor det skisseres en løsning med skjellig grunn til mistanke om straffbart forhold, men ikke at det må knytte seg til en bestemt person. Et ytterligere vilkår om at tvangsmiddelet vil være av vesentlig betydning for etterforskingen vil antagelig være å leve med selv om det vil bety en klar innskjerping i forhold til dagens lovhjemmel.

Høringsbrevet tar opp overskuddsinformasjon. Dette er et langt mindre problem ved trafikkdata/lokaliseringsdata enn for eksempel KK. Det nasjonale statsadvokatembetet har ingen erfaring med at overskuddsinformasjon fra trafikkdata fører til tiltale med mindre det er en solid sak fra før. Dette i motsetning til KK, hvor typisk innholdet i samtalen i enkelte tilfelle vil kunne være nok.

6.2 Hvilke data som skal lagres

NAST bekrefter behovet for å lagre alle opplysningene som er nevnt i forslaget til ekomlov § 2-8 annet ledd. Den saklige avgrensningen av lagringsplikten som følger av at den knyttes til tilbyderbegrepet i ekomloven § 1-5 nr. 14, synes å være hensiktsmessig, selv om det utelukker lagring for en rekke praktiske tjenester som webmail og internettkafeer. Det er bra at det legges opp til en fortløpende vurdering av behovet for eventuelt å utvide lagringsplikten til å omfatte flere tjenester, med hjemmel i forskrift og enkeltvedtak (høringsnotatet pkt. 4.6 s. 33-34).

NAST reiser spørsmål ved om den avgrensning av tjenester som følger av lovens tilbyderbegrep i seg selv burde anses å være tilstrekkelig. Ifølge høringsnotatet legges det vekt på hensynet til teknologinøytralitet, men den foreslåtte utformingen av ekomloven § 2-8 annet ledd begrenser virkningen fordi opplistingen fullt ut er tjenestespesifikk, jf. "fasttelefoni, mobiltelefoni,

internettelefoni, internettaksess og e-post". NAST foreslår at lovgiver erstatter opplistingen med "elektroniske kommunikasjonstjenester", eller henger det på som et alternativ etter opplistingen, for eksempel slik: *"... og andre elektroniske kommunikasjonstjenester"*.

Det vil kunne fange opp kommunikasjonstjenester som det etter prinsippet om teknologinøytralitet er naturlig å likestille i forhold til lagringsplikten, men som kan falle utenfor fordi man ikke har tenkt på dem i dag. Satelittelefoni er et eksempel, dersom slik kommunikasjon ikke alt er dekket av "mobiltelefoni".

For ordens skyld nevnes det at selv om eksemplene i denne høringsuttalelsen punkt 2.3 bare nevner internettaksess og mobiltelefoni, er det behov for lagring av data knyttet til *alle* tjenestene. Lovbrytere søker å utnytte kommunikasjonstjenester som gir anonymitet. Bruken av anonyme mobiltelefonabonnement bekrefter det, og bruken av klonede mobiltelefoner før det. Da var det knapt lovbrytere som brukte mobiltelefon med registrert abonnement. De vil derfor veksle mellom forskjellige tjenester, noe lagringsplikten må dekke opp.

Lagringssted
Spørsmålet om lagringssted reiser to viktige temaer for politiet. Det ene gjelder hvorvidt dataene bør lagres lokalt eller sentralt. Det andre gjelder forholdet mellom lagringsplikten og besittelsesvilkåret i strpl. § 210.

6.3 Sentralt eller lokalt?

Høringsnotatet stiller tilbyderne fritt i forhold til om de ønsker å lagre dataene lokalt eller sentralt, dvs. hos en tredjepart. Aktøren kan være en av de store tilbyderne eller en uavhengig instans. Den hører uansett ikke inn under politiet.

NAST mener at datalagringens legitimitet best ivaretas ved at dataene lagres hos en aktør utenfor politiet, og lagringen må skje under så betryggende forhold som mulig. NAST antar at den sikreste og ryddigste ordningen er å lagre alle dataene hos én aktør. For politiet vil det forenkle innhenting av opplysningene. Det ligger ikke noe sikkerhetselement i at politiet som i dag, må henvende seg til forskjellige tilbydere. Det bare forsinker etterforskingen. Sentral datalagring gir klar ansvarsplassering mht hvem som er den behandlingsansvarlige, forenkler kontroll og tilsyn med ordningen og oppfyller formålet på beste måte.

Prinsipielt mener NAST at spørsmål om datasikkerheten hos tilbyderne ikke bør være noe argument ved valg av lagringssted. Som enhver annen forretningsdrivende må tilbyder behandle sine data profesjonelt og i samsvar med lovverket. Men hvis det virkelig er slik at man må påregne at bransjen ikke kan håndtere dataene forsvarlig, styrkes jo argumentet for sentral datalagring. Det frigjør også ressurser som i dag går med hos tilbyderne til å betjene politiets utleveringsbegjæringer. Ved sentral lagring er det også mulig å ta i bruk *personvernøkende teknologi* for å beskytte *alle dataene* på et godt nivå. NAST savner en vurdering i høringsbrevet om bruk av slik teknologi ville styrke forslaget om sentral datalagring. Det må anses å være enklest, rimeligst og best oppfylle formålet med datalagring.

Besittelsesbegrepet i strpl. § 210 og lagring i Norge
NAST synes det er noe uklart om lagringsplikten gjelder dataene uansett om de er generert i Norge eller i utlandet, og om besittelsesvilkåret i strpl. § 210 er oppfylt uansett hvor dataene er lagret. Dette er viktig for tilgang til data ved internettbruk. Politiet har opplevd å bli møtt med innsigelse fra ISP om at utleveringsplikten ikke lar seg oppfylle, fordi den tjenesten som ISPen tilbyr ("fronter") i Norge, genererer data fra en tjeneste som ytes av en underleverandør, eller

dataene lagres hos morselskap i utlandet. Politiet har da vært henvist til bruk av rettsanmodning til utlandet, noe som selvsagt hever terskelen for strafforfølgning vesentlig. Se også *Sunde (2006) Lov og rett i cyberspace* s. 289-290 om denne problemstillingen

I høringsnotatet står det at "...Ethvert pålegg overfor tilbyderne om å skulle lagre på norsk territorium vil etter forholdene kunne ses som en begrensning til prinsippet om fri flyt av data innen EØS-området." (høringsbrevet pkt. 4.7.4.5 s. 38).

De konkurranserettslige og de straffeprosessuelle spørsmål bør holdes atskilt. Formålet med datalagring tilsier at man følger det prinsipp at *data som genereres ved en tjeneste fra norsk tilbyder, må anses å være i vedkommendes besittelse*, jf. strpl. § 210. Hvorvidt dataene som genereres er lagret i Norge eller utlandet rent fysisk, fordi man har med underleverandører eller internasjonale konsernforhold å gjøre, har i dagens online-samfunn ingen betydning. Tilbyderen må pålegges å innrette seg slik at vedkommende kan disponere over dataene for å oppfylle utleveringsplikten. Nøyaktig hva som lagres hvor, bør således anses underordnet i forhold til *besittelsesvilkåret*, som gjelder om tilbyder har *faktisk rådighet* over dataene.

Dersom datalagring skjer sentralt oppstår det ikke noe problem i forhold til besittelsesvilkåret, noe som i seg selv taler for å gå inn for sentral lagring. Men det må følge klart av regelverket at også data som ytes av underleverandør m.v., omfattes. Dersom lagring skjer desentralt må det i tillegg presiseres at tilbyder anses å være i besittelse av de opplysninger som lagringsplikten omfatter. Det kan gjøres ved en tilføyelse i strpl. § 210 for eksempel slik: *"Tilbydere anses å være i besittelse av de lagringspliktige dataene uavhengig av hvor de fysisk er lagret."*

6.4 Typer av lovbrudd som kan begrunne utlevering

Det vises til forslaget til innarbeidet liste i strpl. § 210. Bestemmelsen omfatter handlinger som kan medføre straff av fengsel i 3 år eller mer og noen spesielt oppregnede lovbrudd. Departementet ønsker tilbakemelding på denne listen. NAST har bare noen få merknader:

Bestemmelsen om "grooming" er omfattet og strafferammen er fengsel inntil 1 år, jf. strl. § 201 a. Infiltrasjon på nettet for oppklaring av denne type lovbrudd, er en særs krevende fremgangsmåte. Formålet er å avdekke identiteten til personer som avtaler møter med mindreårige for å begå seksuelle overgrep, men veien frem dit er lang og kronglete, noe som skyldes bestemmelsens hensiktskrav. Vanlig modus for slike personer er at de tilbyr en iPhone eller lignende, mot at den mindreårige utfører seksuelle tjenester for dem. Dette oppfyller ikke hensiktskravet etter "grooming"-bestemmelsen, men er seksuelt krenkende atferd etter strl. § 201, som også har 1 års strafferamme. En mulig tilnærming til disse sakene er å foreta ransaking og beslag med grunnlag i siktelse etter strl. § 201. Dette kan gjøres hyppig og muligens skape en almennpreventiv effekt. Men da må strl. § 201 på listen av lovbrudd i strpl. § 210, fordi sporingsinformasjon er nødvendig for å avdekke identitet og ransakingssted.

Åndsverkloven § 54 er en bestemmelse hvor det er behov, men hvor det kan reises spørsmål om bestemmelsen oppfyller kravet til alvorlig nok kriminalitet for trafikkdata.
Musikkbransjen har forgjeves forsøkt å få sperret nettadresser og brukere som tilgjengeliggjør musikk i strid med åndsverkloven. Dersom lovgiver ikke innfører hjemmel for sperring som nevnt, kan rettighetsvernet bare effektiviseres med strafforfølgning. Åvl. § 54 bør i så fall vurderes inntatt på listen i strpl. § 210 fordi man er avhengig av sporingsinformasjon for å kunne oppklare slike forhold. Den har per i dag 3 måneder strafferamme, men fengsel inntil 3 år ved særlig skjerpende omstendigheter.

6.5 Utlevering av data

Praksis i politiet varierer med hensyn til hvilket hjemmelsgrunnlag som brukes for utlevering av abonnementsdata som gir grunnlag for å avdekke lovbryterens identitet. Både strpl. § 203, 210 og ekomloven § 2-9 tredje ledd brukes.

Så vidt forstås går lovforslaget ut på at abonnementsdata skal utleveres med hjemmel i ekomloven § 2-9 tredje ledd. NAST legger derfor til grunn at bestemmelsen slik som tidligere, gir hjemmel for utlevering av opplysninger på grunnlag av forespørsler om abonnementsdata, der grunnlaget blant annet kan være
IP-adresse + tidspunkt (smlg. Rt. 1999 s. 1944 og Rt. 2000 s. 169).
Kontantkort
SIM-kort
Imei-nummer
IMSI-nummer.

Videre legges det til grunn at bestemmelsen fortsatt gir hjemmel for utlevering av historiske abonnementsdata knyttet til en kommunikasjonsadresse, for eksempel abonnenter til et fast telefonnummer.

NAST støtter forenklingen ved at det ikke lenger vil være behov for innhenting avsamtykke fra Post- og teletilsynet, jf. strpl. § 118.

6.6 Påtalemyndighetens hastekompetanse

Påtalemyndighetens hastekompetanse må imidlertid ikke fjernes, slik det legges opp til i høringsnotatet. Det foreligger et klart behov for hastekompetanse, og det er uheldig å måtte henvises til det noe uklare nødrettsgrunnlaget som tilbyder i praksis overprøver. Domstolen fører uansett kontroll med beslutningene i etterkant. Hvis en annen instans enn politi/påtalemyndighet skal godkjenne innhenting av dataene, er det behov for en hastekompetanse for de tilfeller der behovet oppstår brått for eksempel under en aksjon kveld/natt/helg hvor en må innhente data for å pågripe en person. Dette kan typisk ha bakgrunn i en utenlandsk rettsanmodning.

Det er da meget uheldig å måtte vente til neste kontordag.

Det er her verdt å merke seg at politiet kan utføre både romavlyttning og kommunikasjonskontroll ved bruk av hastekompetansen. Det vil være lite symmetri i lovverket hvis innhenting av trafikkdata ikke har en slik mulighet.

En slik hastekompetanse er også, på grunn av plutselige rettsanmodninger fra utlandet, viktig for det internasjonale politi- og påtale samarbeid.

6.7 Lagringstiden

Avveiningen mellom effektivitetshensyn og personvern gjør seg først og fremst gjeldende for spørsmålet om lagringstidens lengde. Som bl.a. "Broken Lorry"-saken viser korresponderer oppklaringsmuligheten ofte med lagringstidens lengde.

Fra politiets ståsted er det selvsagt mest formålstjenlig med lengst mulig lagringstid, dvs. to år. Det viktigste er imidlertid lagringsplikten som sådan, og det er kanskje naturlig å legge seg på den lagringstiden som flertallet av de europeiske statene har valgt, nemlig ett år, jf. høringsnotatet pkt. 3.4.

Det reflekterer at Norge som et heldig land, i det store og hele *foreløpig* har gått klar av terrorproblemer, men i likhet med andre europeiske land har store utfordringer med grenseoverskridende organisert kriminalitet og nettbasert kriminalitet. Det tilsier en lagringstid på minst ett år.

Med hilsen

Siri S. Frigaard

Jan F. Glent

Kopi; Riksadvokaten