



MOTTATT

14 APR 2010

POLITIET

POLITIDIREKTORATET

Det kongelige samferdselsdepartement
Postboks 8010 Dep
0030 OSLO

Deres referanse
09/585

Vår referanse
2010/00134-5 008

Dato
12.04.2010

Høring om datalagring

Vi viser til departementets høringsbrev av 8. januar 2010 om ovennevnte.

Politidirektoratet har forelagt høringen for politimestrene og sjef for særorganer. Vi har innen fristen mottatt uttalelse fra Asker og Bærum, Follo, Gudbrandsdal, Romerike, Oslo, Salten, Haugaland og Sunnhordaland, Sogn og Fjordane, Søndre Buskerud, Telemark, Troms, Hordaland, Østfold, Nord-Trøndelag, Helgeland og Nordmøre og Romsdal politidistrikt, samt fra Politiets data- og materieltjeneste og Politihøgskolen, hvorav sistnevnte ikke har merknader til høringen. Hørings svarene er i noen sammenheng innarbeidet i direktoratets uttalelse. I andre sammenhenger er det henvist direkte til disse. Svarene fra underliggende instanser følger vedlagt i kopi.

Politidirektoratet er kjent med at Kripos og Økokrim har avgitt egne høringsuttalelser direkte til departementet. Direktoratet vil i noen grad henvise til høringsuttalelsen fra Kripos.

1. Sammendrag

Datalagringsdirektivet reiser viktige spørsmål om avveiningen av personvern hensyn opp mot samfunnets behov for å bekjempe kriminalitet.

Direktivet fastsetter en plikt til lagring av trafikkdata, lokaliseringsdata og abonnements/brukerdata fremkommet ved bruk av fasttelefon, mobiltelefon, internettaksess, e-post og bredbåndstelefon. Lagringsplikten skal gjelde for tilbyder av offentlig elektronisk kommunikasjonsnett- eller tjeneste. Innholdet i kommunikasjonen lagres *ikke*. Lagringsplikten innebærer ingen overvåking i egentlig forstand. Trafikkdataene skal oppbevares i en begrenset tid og i henhold til høringsnotatet skal de sikres mot "uautorisert eller ulovlig lagring, behandling, tilgjengeliggjøring eller utlevering. Videre er det kun autorisert personell som skal ha tilgang til dataene". Politiet skal ikke ha tilgang til disse. Det er først under etterforskning av en konkret alvorlig straffesak politiet etter nærmere prosedyrer kan få tilgang til avgrensede trafikkdata knyttet til bestemte personer, hendelser eller åsteder.

Politidirektoratet

Post: Postboks 8051 Dep., 0031 Oslo
Besøk: Hammersborggata 12
Tlf: 23 36 41 00 Faks: 23 36 42 96
E-post: politidirektoratet@politiet.no

Org. nr.: 982 531 950 mva
Bankgiro: 7694.05.02388

Lagring av trafikkdata er ikke noe nytt. Teletilbydere har gjennom flere år lagret trafikkdata for fakturerings- eller kommunikasjonsformål. Politiet har hjemmel til å få tilgang til data som er lagret, og har benyttet trafikkdata som bevis i straffesaker fra 1990-tallet og frem til dags dato. Politiets bruk av slike data under etterforskning, redningsoperasjoner m.v. har så vidt vites ikke vært kritisert. Ekomloven, som trådte i kraft i 2003, oppstiller imidlertid en sletteplikt for tilbyder når trafikkdata ikke er nødvendige for fakturerings- eller kommunikasjonsformål. Endringer i markedet vil med stor sannsynlighet medføre at tilbydernes behov for å lagre trafikkdata av faktureringshensyn vil bli redusert i tiden fremover. Disse endringene medfører at politiet mister den tilgang til trafikkdata som de hittil har hatt.

Det nye med datalagringsdirektivet ligger i at datalagring skal ivareta et kriminalitetsbekjempelsesformål i tillegg til teletilbyders fakturerings- eller kommunikasjonsformål som i dag.

Politidirektoratet erkjenner at lagring av trafikkdata kan oppleves som en krenkelse av personvernet all den stund det store flertall benytter seg av elektroniske kommunikasjonstjenester. Politidirektoratet er enig i at lagring utgjør et inngrep i personvernet, men viser til at inngrepet har en begrenset rekkevidde og stor positiv samfunnsmessig betydning. Den teknologiske utviklingen går samtidig fremover med stormskritt. Når samfunnet utvikler seg, må nødvendigvis politiet gjøre det samme. Politiet må ha adgang til de steder kriminaliteten foregår og adgang til de verktøy kriminelle benytter. Manglende lagring vil i mange tilfeller innebære en myndighetsgodkjent automatisk fjerning av åsted, spor og verktøy.

Med hus kom innbruddstyver, med pengesedler kom pengefalsk, med toget kom togrøverier, med bilen kom promillekjøring og med velferdsstaten kom trygdebedragerier. Kriminaliteten følger samfunnsutviklingen og politiet må følge kriminalitetsutviklingen. Utviklingen av internett har gitt borgerne en ny arena, et sted man kan møtes, snakke sammen, handle med hverandre, forvalte offentlige tjenester og mye annet. Mobiltelefonen har medført at vi kan ringe hverandre nær sagt uansett hvor vi befinner oss. Den nye teknologien er bra for borgerne og gir oss nye og mer effektive måter å kommunisere på. Med den nye teknologien følger dessverre også ny kriminalitet, nye måter å begå eksisterende kriminalitet på, og nye hjelpemidler til å begå "gammel" kriminalitet. Med disse negative sider av utviklingen er det avgjørende at politiet ikke blir avskåret fra å innhente bevis som eksisterer som følge av den samme utviklingen.

Den teknologiske utviklingen har medført at enkeltindividet legger igjen mange flere spor av sine aktiviteter enn i tidligere tider. Man kan mislike denne siden ved den teknologiske utviklingen. Det vil imidlertid være et ikke ubetydelig paradoks dersom samfunnsutviklingen gjøres til et avgjørende argument for at politiet ikke skal kunne ha de nødvendige virkemidler for å bekjempe kriminalitet som utspiller seg på nettopp den nye arena som er et sentralt element i samfunnsutviklingen.

Spørsmålet om å innføre Datalagringsdirektivet eller ikke, er på mange måter et spørsmål om politiet skal få anledning til å bekjempe kriminaliteten på en effektiv måte, eller om bruk av internett og (mobil)telefon skal utgjøre et etterforskningsfritt område for de kriminelle. Manglende lagring av trafikkdata vil innebære noe prinsipielt nytt i norsk kriminaletterforskning. Manglende lagring innebærer at åsted, verktøy og spor i forbindelse med kriminelle handlinger utslettes. Et overgrep mot et barn foretatt på soverommet vil

kunne etterlate spor som vel kan forsøkes fjernet, men det krever en aktiv handling fra overgriperens side. Ved et overgrep foretatt via web-kamera over internett utgjør selve kommunikasjonen det objektive beviset forforbrytelsen: Uten lagring vil beviset for overgrepet kun være tilgjengelig i barnets traume og i gjerningsmannens sinn.

Teknologiutviklingen har medført en kraftig økning i bruken av internettbaserte tjenester og kommunikasjonsformer. Man ser følgelig en tilsvarende økning i kriminalitet som i sin helhet skjer på internett eller ved misbruk av internettbaserte tjenester og kommunikasjonsformer. Eksempler på dette kan være datainnbrudd, dataskadeverk, nettbankbedragerier, kredittkortbedragerier, ID-misbruk, anonyme trusler og sjikane. I de fleste sammenhenger blir dette omtalt som datakriminalitet. Datakriminalitet skiller seg helt fra de andre sakstyper ved at den kriminelle handlingen foregår på det elektroniske mediet selv. I noen typer kriminalitet er det selve kommunikasjonen som kan være det eneste som skiller en straffbar handling fra en lovlig handel. Eksempelvis nevnes verdipapirkriminalitet, ulovlig innsidehandel og ulovlig prissamarbeid. Trafikkdata blir ofte det eneste mulige objektive beviset som er tilgjengelig for politiet. Overgrepssaker på internett, datakriminalitet og hvitsnippforbrytelser er etter sin art svært ulike av natur, men har det til felles at trafikkdata er så sentralt i den etterforskning at vi må stille oss spørsmålet om det i det hele tatt vil være mulig å etterforske disse sakene uten at teletilbyderne pålegges å lagre trafikkdata. I debatten i Norge kan det virke som om mange av aktørene, i iver etter å fremme aktverdige personvern hensyn, har mistet av syne dette perspektivet.

Grunnlovens § 102 setter forbud mot husinkvisisjoner med unntak for kriminelle tilfeller. Det er et grunnleggende prinsipp i norsk rett at myndighetene ikke vilkårlig skal bryte seg inn i den private sfære uten hjemmel i lov. Inngrep skal være begrunnet og skal bare skje etter bestemte prosedyrer, ofte under domstolens kontroll. En persons hus eller hjem kan brukes til å begå straffbare handlinger, eksempelvis overgrep mot barn. Man kan skjule utbyttet fra kriminelle handlinger i huset, for eksempel tyvegods og man kan bruke huset til kriminelle handlinger ved å planlegge forbrytelsen der, gjerne sammen med andre. For at politi- og påtalemyndighet skal kunne oppklare og iredreføre forbrytelser, er det gitt adgang etter nærmere regler til at politiet kan trenge seg inn i folks private hjem. Politiet kan finne spor etter forbrytelser foretatt i huset, eksempelvis blod eller spor av forbrytelser planlagt i huset i form av dokumenter eller andre bevis. Utbyttet fra en kriminell handling kan ligge bortgjemt i husets kjeller. Uten lagring av trafikkdata gjør man i realiteten internett til et "hus" politiet i all hovedsak ikke har tilgang til, selv om det foreligger mistanke om (alvorlige) kriminelle handlinger.

Det fremheves ofte som et argument at forbryterne alltid finner nye veier og at politiet henger etter utviklingen. Politidirektoratet er enig i at det er ønskelig at politiet oftere kunne være i forkant av utviklingen, men politiet kan ikke i noe tilfelle la være å løpe etter.

Vi vil her slutte oss til Salten politidistrikt som uttaler:

"Vi vil ikke bagatellisere frykten for et "overvåkningssamfunn", og behovet for et sterkt personvern. Men for oss som til daglig ser konsekvensene av kriminalitet blir for eksempel "ubehaget" borgerne kan føle ved å vite at noen sitter med denne informasjonen en mer "teoretisk trussel", enn de konsekvensene av alvorlig kriminalitet vi ser til daglig, de overgrepssbildene vi faktisk har foran oss."

Personvern hensyn er en sentral verdi i et demokratisk samfunn som må avveies mot andre viktige samfunnshensyn, som hensynet til kriminalitetsbekjempelse. Det må derfor foretas

en forholdsmessighetsvurdering, og et viktig punkt blir om lagring av data er *nødvendig* for å bekjempe alvorlig kriminalitet og ivareta den nasjonale sikkerheten. Høringssvarene fra politidistriktene og Kripos viser at trafikkdata er helt nødvendig for politiets mulighet til å bekjempe alvorlig kriminalitet. Politidirektoratet mener at innføring av en lagringsplikt for trafikkdata ikke er uforholdsmessig satt opp mot de rettsgoder som lagringen medfører for samfunnet og den enkeltes beskyttelse mot overgrep fra kriminelle.

2 Nærmere om de sentrale hensyn

2.1 Personvern

Politiets oppgaver er nedfelt i politiloven, hvor det i § 1 andre ledd står "politiet skal gjennom forebyggende, håndhevende og hjelpende virksomhet være et ledd i samfunnets samlede innsats for å fremme og befeste borgernes rettssikkerhet, trygghet og alminnelige velferd for øvrig". Bestemmelsen angir de oppgaver politiet har i samfunnet, men understreker også at politiet skal fremme og befeste borgernes rettssikkerhet.

Personvernkommisjonen (NOU 2009:1 s 32 - 33) påpeker at personvern og rettssikkerhet er to grunnleggende komponenter i en rettsstat. Begrepet rettssikkerhet er tradisjonelt knyttet til forholdet mellom enkeltindividet og staten og står sentralt innenfor forvaltningsretten og strafferetten. Personvern og rettssikkerhet vil i mange tilfeller overlappe hverandre - begge har som formål å beskytte individets integritet mot overgrep. Personvern- og rettssikkerhetshensyn vil imidlertid ikke alltid være sammenfallende på strafferettens område. Personvernkommisjonen gir som eksempel at utøvelse av prinsippet om fri bevisførsel kan medføre integritetskrenkelser, for eksempel ved at retten tillater opplasing av private dagbøker eller lignende. I slike tilfeller ser man at rettssikkerheten fordrer at personvernet settes helt eller delvis tilside.

Personvernensyn er som nevnt en verdi i et demokratisk samfunn som må avveies mot andre viktige samfunnshensyn, som hensynet til kriminalitetsbekjempelse. EMK artikkel 8 annet ledd åpner for at det kan gjøres inngrep i personvernet. For at et slikt inngrep skal være forsvarlig må det blant annet være nødvendig i et demokratisk samfunn. Inngrepet som gjøres må være proposjonalt i forhold til formålet som ønskes oppnådd.

Det er Politidirektoratets oppfatning at en lagring av trafikkdata er et beskjedent tiltak i forhold til den lagring av personopplysninger som allerede finnes i dag. Eksempelvis nevnes bankkorttransaksjoner, elektronisk registrering i bomringer og elektroniske billetter innen samferdsel, samt lagring av sensitive personopplysninger hos forsikringsselskap. Metodekontrollutvalget uttaler på side 23 at *"politiets bruk av skjulte tvingemidler utgjør en minimal del av den samlede "overvåking" som til enhver tid foregår i Norge sammenliknet med den generelle kontrollen som utøves ved bruk av observasjon og registrering uten at det foreligger noen konkret mistanke om straffbare handlinger"*. At trafikkdata vil utgjøre et begrenset supplement til denne mengden, mener vi må være av betydning ved vurderingen om lagringsplikt vil være et forholdsmessig tiltak. Metodekontrollutvalget sier videre, på side 22: *"Utralgets undersøkelser viser at politiet forholdsvis ofte innhenter opplysninger om teletrafikk (trafikkdata) som ledd i etterforskning, og at slike data må antas å ha betydning i minimum 40 prosent av sakene de innhentes i. I lys av at innhenting av slike data etter utvalgets vurdering utgjør et langt mindre inngrep i mistenktes og andres personvern enn kommunikasjonsavlytting, er dette etter utvalgets oppfatning tilfredsstillende"*.

Eksempelene i punkt 2.2.1 viser at trafikkdata har stor betydning for politiets mulighet til å bekjempe alvorlig kriminalitet. Etter Politidirektoratets oppfatning utgjør lagringen et forholdsvis begrenset inngrep i personvernet og er nødvendig for å beskytte samfunnet mot alvorlige former for kriminalitet

2.2 Politiets behov for trafikkdata i etterforskning

Kommunikasjonen innenfor mer eller mindre organiserte nettverk er et viktig verktøy for stadig flere kriminelle.

Romerike politidistrikt uttaler at det i flere alvorlige straffesaker er avdekket at bevisene for det straffbare forholdet i seg selv ligger i opplysninger fra trafikkdata. Organiserte kriminelle forsøker å skape avstand i tid og sted mellom seg selv og den straffbare handlingen. Kontakten mellom bakmannen og personen som utøver selve handlingen hadde således ikke latt seg bevisføre uten tilgang til trafikkdata. I andre saker har tilgang til trafikkdata gjort politiet i stand til å gå tilbake i tid og rekonstruere kontakten gjerningsmennene har hatt med hverandre (personspesifikke spor) samt dokumentere hvilke basestasjoner de har vært tilknyttet (stedsspesifikke spor), ofte i strid med deres egne forklaringer. Flere av de øvrige politidistriktene peker på tilsvarende.

Det er ikke gjort noen undersøkelse for å se på nytteverdien av bruk av trafikkdata i etterforskningen i forbindelse med høringsnotatet til datalagringsdirektivet. Vi registrerer at Metodekontrollutvalget (NOU 2009:15 s. 116 - 177) har lagt til grunn at trafikkdata har vært til nytte i etterforskningen i minst 40% av sakene hvor trafikkdata er innhentet.

Kripos har foretatt to undersøkelser som gjelder henholdsvis nytteverdi av trafikkdata i etterforskningen og omfang av politiets bruk av trafikkdata.

I den ene undersøkelsen så Kripos på bruk av trafikkdata i utvalgte sakstyper fra 2008 som har ført til en positiv påtaleavgjørelse. Resultatet viser at det ble innhentet trafikkdata i ca 52 % av de undersøkte sakene. Tallene viser videre at ca 82% av dem som innhentet trafikkdata etter en politifaglig vurdering var enige i at opplysningene hadde stor betydning for etterforskningen.

I den andre undersøkelsen innhentet Kripos statistikk hos teletilbydere som viser politiets bruk av trafikkdata i perioden 2007-2009. Tallene viser at politiet i denne perioden innhentet ca 4.600- 5.000 utskrifter pr år fra konkrete telefonnummer. Utskrifter fra basestasjoner ble innhentet i ca 250 tilfeller i 2007 og ca 300 tilfeller i 2008 og 2009. For videre detaljer om undersøkelsene, viser vi til høringsuttalelsen fra Kripos.

I årene 2007 – 2009 ble det årlig registrert i underkant av 400.000 anmeldelser. I en straffesak er det vanlig at det innhentes trafikkdata fra flere telefonnummer. Med andre ord vil ikke antallet utskrifter korrespondere med antall saker man innhenter data i. Trafikkdata innhentes således i et relativt lite antall saker, men de har meget stor betydning i de sakene de faktisk innhentes.

2.2.1 Eksempler på saker/ sakstyper

I dette punktet vil vi gi noen eksempler på konkrete saker hvor trafikkdata har hatt stor bevismessig betydning for etterforskning og dom. Vi viser også et par eksempler på saker hvor mangelen på trafikkdata har hatt stor betydning og hvordan lagringstidens lengde får betydning for politiets oppklaringsmulighet.

Politidirektoratet viser her noen eksempler, men viser for øvrig til høringsuttalelsene fra politidistriktene og Kripas.

Narkotika

Trafikkdata er svært viktig i samtlige av sakstypene innen organisert kriminalitet, eksempelvis narkotikakriminalitet og menneskehandel. Etterforskningen retter seg ofte mot bakmenn i Norge og utlandet, som benytter et omfattende nettverk som stråmenn. Kommunikasjon står sentralt også i de kriminelle nettverkene, og elektroniske spor er svært ofte avgjørende for å vise knytningene i miljøet og bevegelser/lokalisering på gjerningstidspunktet. Slik etterforskning, spesielt over landegrensene, er svært tidkrevende, og teleleverandørenes lagringstid er ofte overskredet når etterforskningen løpende avdekker sentrale aktører.

Eksempler:

Innførsel og omsetning av flere kilo heroin 1999 – 2000 (Romerike pd).

Gjennom spaning og kommunikasjonskontroll avdekker politiet innførsel av 5 kilo heroin knyttet til et utenlandsk nettverk, tilreisende utlendinger midlertidig bosatt på Romerike og et pakistansk nettverk på Romerike. Trafikkdata bakover i tid avdekker ennå 2 innførsler av heroin der modus, kontaktmønster og reiser er lik den avdekkede innførselen. Bevisene fra trafikkdata viser hovedmennenes roller over tid og medfører domfellelse av hovedmenn, kurer og mottagere i Norge. Hovedmennene får 15 og 16 års ubetinget fengsel. Rolleforståelse, organisering og handlingsmønster over tid hadde ikke blitt avdekket uten trafikkdata.

Funn av til sammen 28 kilo amfetamin i Fetsund 2004 (Romerike pd).

Lensmannen i Fet og Rælingen på Romerike rykker ut til en gård der det er meldt om skyting. Stedet er forlatt. På stedet finner han 28 kilo amfetamin i en fryseboks. På stedet finner man en rekke mobiltelefoner og SIM-kort. Ingen av disse er registrert på personer. Avhør av vitner og annen etterforskning avdekker 2 aktuelle personer til huset der narkotikaen blir funnet. Begge er godt kjent av politiet for grov narkotikakriminalitet fra tidligere. Ved innhenting av trafikkdata klarer politiet å binde 3 helt andre personer til partiet med narkotika. Lagrede tekstmeldinger på beslaglagte telefoner avdekker handlingene. Sammenholdte trafikkdata mellom gjerningsmennenes registrerte åpne telefoner og telefonene funnet på gården knyttet de mistenkte til disse telefonene og avdekker ytterligere innførsel og omsetning av til sammen 250 kilo hasj og 40 kilo med amfetamin. Hovedmannen blir dømt til 15 års fengsel. Innhentede trafikkdata var helt avgjørende som bevis i saken. De innhentede trafikkdataene viste videre at de 2 personene som først var siktet i saken kun hadde en svært perifer rolle.

Etterforskning av multi-kriminelt nettverk, Romerike politidistrikt 2006 – 2007.

Saken hadde utgangspunkt i en analyse av flere saker der det forelå trafikkdata. Gjennom analysen avdekket politiet et miljø man mente forsynte flere personer og flere nettverk med narkotika, og andre straffbare handlinger. Gjennom den videre etterforskningen beslaglegger Romerike politidistrikt i samarbeid med flere distrikter store partier med narkotika, bl.a. 15 kilo heroin, 40 kilo amfetamin, 50 kilo amfetamin, 100 kilo hasj, 2 kilo amfetamin, 2 kilo amfetamin, 2 kilo kokain samt en rekke mindre beslag. I tillegg avdekker etterforskningen omsetning av flere kilo heroin i nettverket. Underveis i etterforskningen har politiet innhentet ca 100 utskrifter av teletrafikk. Opplysninger fra teletrafikken har gjort politiet i stand til å avdekke hvordan hovedmennene har kommunisert med hverandre. Opplysninger fra teledata sammenholdt med annen etterforskning var avgjørende bevis i flere av hovedforhandlingene i retten.

Operasjon Laban (Oslo pd)

Kommunikasjonskontroll avdekket overlevering av to kg heroin og at det fantes mer. I etterkant av tilslaget fant man depotet, hvor det ble beslaglagt ca. 17 kg heroin. Trafikkdata på hovedpersonene viste seg å være viktig, idet ikke alle personene inngikk i kommunikasjonskontrollen. Trafikkdata viste knytningene mellom de ulike personene hadde med hverandre. Basestasjonene viste at "løpegutten" ved flere anledninger hadde vært på basestasjonen som dekket adressen for depotet.

De tre domfelte fikk fengselsstraffer på hhv. 15 år og seks måneder, 11 år og åtte år.

To innsatte organiserer innførsel av 2 større amfetaminpartier fra Litauen mens de soner lengre narkotikadommer i Bergen fengsel. (Hordaland pd)

5 personer ble dømt til lengre fengselsstraffer for innførsel av 2 større partier med metamfetamin fra Litauen til Norge. To av gjerningspersonene sonet fengselsstraffer på gjerningstidspunktene. Retten la til grunn at det var de to innsatte i Bergen fengsel som hadde hatt de mest sentrale rollene i innførselen. Trafikkdata var helt sentralt for å bevise knytningene mellom de siktede og kontakten med leverandøren i Litauen. Det ville trolig ikke ville vært tilstrekkelig bevis mot de 2 hovedmennene uten trafikkdata. Leverandøren i Litauen ville ikke blitt avslørt uten de opplysninger som fremkom av innhentet trafikkdata. (Gulating lagmannsretts dom av 10.6.2009)

Menneskehandel

Norge har ved ratifisering av Europarådkonvensjonen mot menneskehandel forpliktet seg til å tilby bistand og beskyttelse til de som identifiseres som mulige ofre for menneskehandel. Blant annet har disse rett til en seks måneders refleksjonsperiode (midlertidig oppholdstillatelse) for å vurdere om de ønsker å anmelde forholdet for politiet. De aller fleste ofre for menneskehandel trenger tid før de velger å anmelde menneskehandel og benytter seg derfor av sin rett til refleksjonsperiode. Dersom anmeldelse blir inngitt har det derfor som regel gått flere måneder siden de[t] anmeldte forhold skjedde. Sentrale elektroniske spor som kunne bekreftet ofrenes historie er gått tapt. Slike spor vil typisk være telefon eller internettbruk som kan gi opplysninger om bakmenns rekruttering og kontroll av ofrene, reiserute, annonsering av tjenester på internett osv. En menneskehandelsak hviler i stor grad på ofrenes vitnemål og uten denne type opplysninger som kan utdype og underbygge ofrenes forklaring, viser det seg ofte svært vanskelig å etterforske og føre tilstrekkelige beviser for menneskehandel.

Eksempel:

Grov Menneskehandel med mindreårig albansk jente (Hordaland pd)

3 personer domfelt for grov menneskehandel. 17 år gammel albansk jente utnyttet til prostitusjon. Trafikkdata var et helt sentralt bevis i saken for å avdekke knytninger mellom de siktede, reiseruter og knytning til fornærmede. Det antas med sikkerhet at ingen av de tiltalte ville blitt domfelt uten det bevismaterialet som ble avdekket gjennom innhenting av trafikkdata. (Gulating lagmannsretts dom av 14.12.2009).

Seksuelle overgrep

I enkelte alvorlige saker får ikke politiet kjennskap til saken før det er gått en tid. Ulike prosedyrer regulerer slike sakers fremvekst og videre behandling. Mange kommuner har opprettet voldtektsmottak hvor offeret kan få sikret biologiske og andre spor fra voldtekten. Dette er spor som lagres ved voldtektsmottaket mens offeret vurderer om saken skal politianmeldes. Det kan gå lang tid fra sporene ble sikret til politiet blir varslet. Når

vedkommende anmelder saken, kan politiet hente sporene på mottaket. Hvis datalagringstiden er kort, vil de ulike trafikkdata som kan ha bevismessig betydning for saken være tapt.

Det er et generelt behov for lagring av trafikkdata i overfallssaker/voldtektssaker med ukjent gjerningsmann, eller moduskandidater i serievoldtektssaker, hvor det ikke forefinnes annet i saken enn fornærmedes forklaring og anmeldelse i tillegg til likhetstrekk og samme modus ved flere gjentakende forhold over tid/flere år. Ved å ha tilgang til basesøk og lagret trafikkdata lenger tilbake i tid enn det som nå er mulig, kunne politiet avdekket om vedkommende befant seg i gitt område på tid og sted for anmeldt forhold. Dermed vil politiet ha et bedre og annet grunnlag for å etterforske videre – enten for å kunne sannsynliggjøre at vedkommende faktisk var i det aktuelle området, eller på den annen side for å kunne fjerne mistanken mot vedkommende i den enkelte sak.

Eksempel:

Omfattende seksuelt misbruk av barn (Hordaland pd)

43 år gammel mann dømt til 10 års forvaring med en minstetid på 6 år for omfattende seksuelt misbruk av barn under 14 år og barn under 16 år, menneskehandel og produksjon av barnepornografi. Trafikkdata ble innhentet for tiltaltes mobiltelefon, for perioden fra løslatelse fra første fengslingsperiode, og frem til ny pågrepelse. Dette ga bevis for fortsatt kriminell virksomhet - misbruk av gutter seksuelt, som igjen ledet til ny pågrepelse og fengsling frem til hovedforhandling grunnet kvalifisert gjentakelsesfare. (Bergen tingretts dom av 14.1.2010)

Hordaland politidistrikt påpeker at det internasjonale samfunn har stor fokus på internettbasert spredning av bilder og filmer av seksuelle overgrep mot barn. Norge har ved flere anledninger deltatt i koordinerte internasjonale aksjoner for å straffeforfølge overgripere og identifisere barn som er utsatt for dokumenterte seksuelle overgrep. Informasjon innhentet fra slike aksjoner kan føre til nye aksjoner for å straffeforfølge andre overgripere og identifisere nye barn, eller skape bedre grunnlag for å identifisere barn. Hvis Norge har kortere datalagringsbestemmelser enn samarbeidende nasjoner, står Norge i fare for å utelukke seg selv fra slikt samarbeid. Norge står også i fare for å bli en hemske for andre nasjoners bestrebelser på å avdekke overgripere og identifisere barn som utsettes for seksuelle overgrep. Det vil åpenbart være grunn til å frykte at slikt materiale vil være tilgjengelig på eller via servere i Norge, fordi trafikkdata ikke vil være lagret her. Man har for øvrig sett internasjonalt at kriminelle organisasjoner/nettverk er svært dyktige i å tilpasse seg den til enhver tid gjeldende lovgivning, herunder de endringer som blir gjort.

Salten politidistrikt viser til et eksempel hvor det er behov for lengre lagringstid. Eksempelet er fra en alvorlig sak om overgrep mot barn som for tiden er under etterforskning. Overgrepene siktelsen gjelder har en strafferamme på 21 års fengsel. Politidistriktet bemerker at dersom det hadde foregått datalagring i henhold til EUs datalagringsdirektiv, ville saken hatt et mye større omfang i og med at politiet da høyst sannsynlig ville kommet i kontakt med flere ofre. Vi viser her til høringsuttalelsen fra Salten politidistrikt, hvor det blant annet fremkommer følgende:

Problemet oppsto da vi sendte alle Microsofts registrerte ip-adresser videre til teletilbyder. Teletilbyderne har bare anledning til å knytte ip-adressene direkte til en abonnent over en begrenset tidsperiode. Da vi tok kontakt med dem, kunne derfor bare 20 av de 46 e-postkontoene/identene spores tilbake til de eksakte abonnentene der noen hadde vært pålogget

de aktuelle e-postkontoene. De andre ip-adressene var for gamle, siden e-postbrukeren ikke hadde vært på Internettet via MSN eller e-post de siste 21 dagene.

Det gikk relativt få dager fra vi startet etterforskningen av saken, frem til vi kontaktet teletilbyder for å få ut informasjon om hvilke abonnenter som har vært pålogget de aktuelle e-postkontoene. Det er så raskt som et lite politidistrikt som vårt er i stand til å jobbe frem denne typen informasjon. I vårt tilfelle førte dette til at vi måtte ta bort 26 ofre eller mulige ofre fra saken. Vi vet ikke om disse har møtt mannen, om de har vært utsatt for overgrep over Internettet, eller utsatt for andre straffbare handlinger. Vi vet ikke en gang hvem de er.

Vår sak viser hvor viktig det er at kriminalitet blir meldt inn raskest mulig, slik at politiet kan sikre spor, både med tanke på at skyldige ikke skal gå fri, og med tanke på at uskyldige ikke skal dømmes. Tidsrommet for datalagring skal ikke bare være til hjelp for fornærmede, men også for mistenkte. Vi kan dokumentere at siktede i denne saken har begått overgrep for mer enn 10 år siden gjennom beslag av filmmateriale.

Drap

Også i drapssaker kan utskrifter fra fornærmedes telefon være viktig. Trafikkdata viser hvem offeret har vært i kontakt med og offerets bevegelser rett før drapet. I saker med ukjent gjerningsmann vil de stedsspesifikke sporene i form av basestasjonsutskrifter kunne være av avgjørende betydning.

Eksempler:

Dobbeltdrap i Bjerregaardsgata – avgjørende bevis (Oslo pd)

To studenter ble funnet drept på sin felles hybel i Bjerregaardsgata, fredag 20. februar 2004. Det var siktede selv som varslet vaktmester om at han ville inn på hybelen for å sjekke om de var der. Teledata var et sentralt og avgjørende bevis i saken. Siktede sendte en tekstmelding fra en av de fornærmedes telefoner til sin egen telefon etter at de var drept. Undersøkelser hos teleselskapet NetCom viste at simkortet til en av de fornærmedes telefoner har stått i siktede sin telefon ved minst to anledninger.

Drosjedrapet i Nittedal i 1999 (Romerike pd).

Utskrifter fra fornærmedes telefon dokumenterte kontakt med mistenkte i tiden rett forut for selve drapet. Innhentede trafikkdata fra mistenktes telefon knytter ham direkte til handlingen og impliserer ytterligere en person. Begge de to er dømt i saken. Etterforskeren i saken mener de innhentede trafikkdata var helt avgjørende for bevisføringen og at man ikke hadde funnet frem til gjerningsmennene uten trafikkdata.

Drap i Maria Dæhliesvei (Oslo pd).

En person ble funnet drept 29. januar 2009. Flere opplysninger i saken peker mot at drapet fant sted 26.01.09, på kvelden. Trafikkdata fra fornærmede og siktedes telefon viste at de hadde en felles kontakt drapsdagen og vi kunne ut fra siktedes basestasjoner se at han oppholdt seg på drapsstedet da fornærmede ble drept.

Oslo politidistrikt har også gitt eksempler på saker der det hadde vært behov for lengre lagringstid enn i dag:

Drap på Haugerud (behov for lengre langringstid) (Oslo pd)

Drap der siktede etter drapet forsøkte å skjule spor ved å tenne på en bil med offeret i. Etterforskningen har avdekket at det sannsynligvis er et bestillingsdrap. Det tok tid før politiet fant en link mellom siktede og dem han drepte på oppdrag fra, og mye trafikkdata var da gått tapt. Flere av de personene politiet jobber med opererer med flere telefonnummer og det kan gå tid før vi får vite hvilke telefonnummer som er brukt. Tre mnd kan da være alt for kort tid, idet mye trafikkdata går tapt på den tiden.

Nordahl Brunsgate (behov for lengre lagringstid) (Oslo pd)

En person ble funnet drept i Nordahl Brunsgate. Saken står fortsatt med ukjent gjerningsmann... Vi har i dag opplysninger som kunne blitt avkreftet eller bekreftet dersom trafikkdata hadde blitt lagret i en lengre periode.

Ran

Ved grove ran vil stedsspesifikke spor i form av basestasjonsutskrifter være viktig for etterforskningen, da det som regel er ukjent gjerningsmann. Trafikkdata kan gi opplysninger om gjennomføringen og planleggingen av ranet, og hvilke vitner som var på ransstedet.

City-ranet Lillestrøm, 1998. (Romerike pd)

Flere ranere bevæpnet med skarpladde militærvåpen tok seg inn på handlesenter i Lillestrøm om natten. Senere overfalt de og ranet 2 vektere fra et vakselskap som var kommet til stedet for å hente dagens omsetning. Ranet bar preg av planlegging og brutalitet. Innhenting av trafikkdata fra basestasjoner gjorde at politiet kunne knytte flere mellommenn til ranet. Senere etterforskning og innhenting av trafikkdata på disse personene gjorde politiet i stand til å pågripe gjerningsmennene. Hovedpersonene ble dømt til henholdsvis 8 og 9 års fengsel. Uten innhenting av trafikkdata på basestasjonen ville politiets etterforskere ikke hatt muligheter til å avdekke gjerningsmennene.

Vinning

I arbeidet mot mobile vinningskriminelle, særlig når det gjelder grove tyverier fra bolig, har historiske trafikkdata i flere tilfeller vært avgjørende for oppklaring og senere domfellelse i sakene. I mange tilfeller opererer flere sammen i nettverk og det er viktig å få tatt flest mulig av de personene som inngår i nettverkene. Politiet har erfaring med at de involverte ikke innrømmer mer enn det de blir tatt for. Det er derfor helt avgjørende for håndteringen av denne typen saker at politiet kan bruke trafikkdata som et verktøy for å knytte personer sammen og knytte personer til åstedene. Asker og Bærum politidistrikt deltar i samarbeidsprosjektet "Grenseløs", og opplyser at de i mange saker ser at de faktiske opplysningene trafikkdata gir, kan bidra til at siktede erkjenner både forhold og kjennskap til involverte personer. I flere saker vil trafikkdata også være viktig for domfellelse for organisert kriminalitet, jf strl § 60a, og da særlig kravet om organisert kriminell gruppe.

Eksempel:

Omfattende og profesjonell vinningskriminalitet — Prosjekt Albatross (Hordaland pd)

5 personer domfelt for til sammen ca 75 straffbare forhold, fortrinnsvis grove tyverier begått ved tyveriraid fra Lindesnes til Harstad. Trafikkdata var helt avgjørende bevis i saken. Uten trafikkdata ville det ikke vært mulig å knytte de siktede til åstedene. Det ville heller ikke vært mulig å knytte de siktede til hverandre i det omfang som ble avdekket gjennom innhenting av trafikkdata fra beslaglagte mobiltelefoner. Politiet ville ikke hatt bevis for at gjerningsmennene samarbeidet om

tyveriene. Det antas med stor grad av sikkerhet at tilnærmet samtlige forhold ville blitt henlagt uten opplysningene som fremgikk av trafikkdata. (Gulating lagmannsretts dom av 11.4.2007)

Økonomisk kriminalitet

Trafikkdata er sentralt i etterforskingen av økonomisk kriminalitet. I noen typer kriminalitet er det selve kommunikasjonen som kan være det eneste som skiller en straffbar handling fra en lovlig handel. Eksempelvis kan kommunikasjon mellom daglig leder og en "tilfeldig" investerende slektning i dagene før en børskunngjøring være en sterk indikasjon på innsidehandel. Verdipapirkriminalitet er et område som peker seg ut som sårbart dersom man skulle velge å la være å lagre trafikkdata. For denne type kriminalitet vil kommunikasjonen i noen grad alene kunne utgjøre den kriminelle handling og svært ofte vil trafikkdata utgjøre det eneste objektive sporet som kan vise om det har foregått noe kriminelt. Det samme kan man antagelig si om ulovlig prissamarbeid. Kontraktene og dokumentene vil sjelden eller aldri vise at det har foregått et ulovlig samarbeid. Trafikkdata vil ofte være det eneste sporet som kan vise om det har vært kontakt mellom de impliserte.

Oslo politidistrikt opplyser at de erfaringsmessig ikke mottar saker om økonomisk kriminalitet før det har gått en god stund. Det er flere årsaker til dette, men en viktig årsak ligger i at økonomisk kriminalitet kan være vanskelig å oppdage, og det er ikke sjelden at det straffbare forhold kan ligge et halvt til ett år tilbake i tid på det tidspunktet politiet mottar anmeldelse. Lagring av trafikkdata for en lengre periode er således viktig.

Eksempel:

Operasjon Plastic Fantastic (Oslo pd)

Denne saken startet med en rekke bedragerier utført av enkeltpersoner i første halvdel av 2007. Man tappet konti til rike personer med falske kort og falske pass ved at gjerningspersonen gav seg ut for å være "den rike".

I juni 2007 begynte politiet å se en sammenheng mellom sakene og koordinere opplysningene. Det viste seg etter hvert at en organisasjon med flere ledd stod bak. Sommeren 2007 var politiet i posisjon til å hente inn trafikkdata på "første bakmannsledd", som hadde fulgt en del av gjerningspersonene rundt i bankene i forbindelse med at kontoene skulle tappes. Flere av disse bakmennene ble pågrepet og fengslet i dette tidsrommet. Samtlige nektet straffeskyld. Etter å ha analysert trafikkdata for disse bakmennene, fant politiet at de hadde telefonkontakt med gjerningspersonene både før og etter at bedrageriene fant sted. Disse funnene er av avgjørende verdi i saken, all den tid bakmennene selv ikke tilstår.

I løpet av høsten 2007 opplevde man imidlertid at bedrageriene fortsatte med samme modus, til tross for at flere sentrale personer var varetektsfengslet. Etter en ny runde med etterforskning i saken, avdekket politiet våren 2008 produksjon av falske pass, en insider ansatt i DnB Nor og en hovedmann. Dette førte til pågrepelse av en rekke personer i starten av mars 2008. De straffbare forholdene i saken befant seg derimot innenfor året 2007. Innen man hadde avdekket de mest sentrale personene i denne organisasjonen, og ikke minst insidern i DnBNor, hadde det gått for lang tid til at man kunne hente inn trafikkdata som kunne underbygge dagens siktelse som lyder på organisering grove bedragerier etter §60a i straffeloven, samt grov korrupsjon.

Totalt sett har ca 30 personer vært mistenkt eller siktet i saken, som er berammet til høsten 2010.

Forsvinningssaker

Politiet har også behov for trafikkdata i forsvinningssaker. Dette er saker hvor det innledningsvis kan være vanskelig å avgjøre om det foreligger mistanke om et straffbart forhold, og der heller ikke en nødrettslig begrunnelse kan benyttes for å få tilgang til

relevante data. Forslaget i høringsnotatet synes ikke å hjemle utlevering i slike situasjoner, noe som vurderes å være en mangel. Direktivet på sin side åpner opp for utlevering i "særlige saker" og forsvinningssaker synes naturlig å kunne omfattes av dette vilkåret. Det som innledningsvis blir betegnet som en forsvinningssak kan senere vise seg å være en drapssak. Det er meget uheldig om trafikkdata i mellomtiden er blitt slettet. Her vil vi eksempelvis vise til erfaringene som Hordaland politidistrikt gjorde i forbindelse med evalueringen av den såkalte Trine Frantzen-saken. I denne evalueringen fremkommer det at etterforskningen av denne saken som drapssak ble vesentlig vanskeliggjort fordi trafikkdata var slettet før en kom i gang med etterforskningen.

2.2.2 Tilgang på trafikkdata dersom datalagringsdirektivet ikke implementeres

I henhold til praksis fra EMD bør man se hen til om et tiltak kunne vært utført på en mindre inngripende måte. Det er i debatten hevdet at "frysing" av data etter straffeprosessloven § 215a eller kommunikasjonskontroll vil være tilstrekkelige alternativ til lagring.

Tilbakemeldinger fra politidistrikt og særorgan viser at det *ikke* er andre etterforskningsmetoder som kan erstatte tilgang til historiske trafikkdata. De foreslåtte alternativene er mindre egnet ved reaktiv etterforskning. Bortfall av historiske trafikkdata kan også svekke politiets mulighet til å benyttes kommunikasjonskontroll, da det kan være nødvendig i forkant å innhente data for å kunne identifisere det anlegg man ønsker å avlytte.

Oslo politidistrikt bemerker at kortere lagringstid og tap av trafikkdata medfører økt bevismessig behov for andre og presumptivt mer inngripende metoder ut fra personvern hensyn. Eksempelvis nevnes det som i høringsnotatet er betegnet som sanntids kommunikasjonskontroll. Dette vil medføre en stor, og unødvendig, arbeidsbelastning for politiet, påtalemyndigheten og retten, og det vil også være mer inngripende for de impliserte i straffesakene. Hvis vi ikke har trafikkdata på den som avlyttes kan vi komme i en situasjon at vi må avlytte flere personer, noe som er vesentlig mer inngripende og ressurskrevende enn kun å innhente trafikkdata.

Troms politidistrikt påpeker også at endringer i markedet og den teknologiske utviklingen medfører at tilbyderne i mindre utstrekning fremover vil ha behov for å lagre trafikkdata for faktureringsformål. Man står altså overfor en situasjon hvor mangel på lovregulering i nær fremtid vil føre til at nytteverdien av straffeprosessloven § 215a blir liten ved at det ikke finnes data å "fryse"

2.3 Politiets behov for trafikkdata til Redningstjenesten

Utenfor etterforskning innhentes i dag trafikkdata innen redningstjeneste i forbindelse med søk etter savnet person. Data blir ofte innhentet (av HRS eller LRS) på et nødrettslig grunnlag for å lokalisere personer i nød. Redningstjenestens oppgaver er kun å redde mennesker i akutt nød. Trafikkdata innhentes i nåtid – eventuelt fra det tidspunkt en person er meldt savnet. Hovedregelen er at disse trafikkdata er mindre enn en uke gamle – kanskje bare en dag gamle. Søndre Buskerud politidistrikt påpeker at dersom innhenting av trafikkdata skal være særlig aktuelt i denne forbindelse må dette skje så raskt som mulig, slik at liv kan berges. Denne innhenting av trafikkdata går på sporing av i hvilket område mobiltelefonen befinner seg/siste kjente område, og er ofte avgjørende i forhold til organiseringen av leteaksjonen.

I likhet med både Søndre Buskerud og Salten politidistrikt vil vi understreke viktigheten av at man fortsatt må ha tilgang til trafikkdata til redningsformål.

3 Høringsnotatets spørsmål

3.1 Presisering av hva som skal lagres

Utgangspunktet må være at alle data som kan tenkes å ha bevismessig betydning i straffesaker skal lagres.

En klar presisering kan imidlertid være viktig, slik at man unngår at tilbyderne har ulike oppfatninger om hvilke data som skal lagres. Høringsnotatet gir i punkt 4.4.1 – 4.4.5 en presisering av hva som skal lagres. Presiseringene synes i hovedsak å dekke de nødvendige data knyttet til de forskjellige kommunikasjonsformer. Det kan imidlertid være noen uklarheter når det gjelder IP-telefoni og internettaksess. Det bør vurderes om man kan sikre teknologinøytralitet samtidig som bestemmelsene sikrer nødvendig presisjon.

3.2 Lagringstid og forslaget om å skille lagringstid etter teknologi

3.2.1 Forslaget om å skille lagringstid etter teknologi

Politidirektoratet mener at lagringstiden bør være den samme uavhengig av valg av teknologi. Dette synet støttes også av alle politidistrikt som har uttalt seg om spørsmålet. I høringsnotatet er det vist til konkurransehensynet som ett argument for en slik løsning. Vi ser det også som en fordel i politiets kriminalitetsbekjempelse om lagringstiden er den samme for all teknologi som blir benyttet.

Vi slutter oss til Sogn og Fjordane politidistrikt som uttaler:

I forhold til lagringstiden er vi av den oppfatning at det ikke bør skilles på teknologi. Dette begrunnes i at teknologiene går over i hverandre i mange sammenhenger. For eksempel ved at det benyttes mobiltelefon som modem for å gi datamaskin tilgang til Internet. Videre vil eventuelt lovverket være bedre rustet til å fange opp teknologiutviklingen.

3.2.2 Lagringstidens lengde

Hensynet bak datalagringsdirektivet er bekjempelse av alvorlig kriminalitet. Oslo politidistrikt påpeker at etterforskningen i slike saker ofte er komplisert, omfattende og tidkrevende, hvor bakmenn/gjerningspersoner først blir identifisert og mistenkt etter måneder og år med intensiv etterforskning. Med alvorlig og organisert kriminalitet ser vi en økende grad av internasjonal etterforskning, et økende fokus på bakmenn og en større grad av profesjonalitet blant kriminelle. Politidirektoratet ser det derfor slik at man som utgangspunkt ønsker at lagringstiden i direktivet utnyttes fullt ut, dvs en lagringstid på to år. Flere av politidistriktene uttaler at det er behov for en lagringstid på to år;

Oslo politidistrikt:

Dersom reglene skal tjene formålet, må lagringstiden i direktivet utnyttes fullt ut. Lagringen vil skje på betryggende måte, og vil kun gis ut etter beslutning fra kompetent myndighet. En kan følgelig ikke se at en noe lengre lagringstid vil utgjøre en stor forskjell ut i fra personvernens hensyn, og det oppveies av den store betydning lengre lagringstid har for oppklaring av alvorlig kriminalitet... Oslo politidistrikt er derfor av den klare oppfatning at en lovpålagt lagringstid på to år vil være et vesentlig, og nødvendig, bidrag til bekjempelsen av alvorlig kriminalitet.

Gudbrandsdal politidistrikt:

Det er flere sakstyper hvor en etterforskning ikke vil starte før det har gått en viss tid. Spesielt kan dette gjelde i forsvinningssaker for eksempel "Lena-saken" og ved spredning av barnepornografi. Lagringstiden bør således være av en viss lengde. Passende lengde antas å være to år.

Telemark politidistrikt:

Ved etterforskning av nettverk og kriminalitet som pågår over tid, vil nye mistenkte ofte "dukke opp" underveis i etterforskningen. Det krever at data er lagret slik at også etterforskningen av nye mistenkte kan bli rask og effektiv. Vår oppfatning er at 12 måneders lagringstid vil kunne være for lite i slike tilfeller... Etter vår oppfatning vil automatisk lagring i to år innebære at data i gitte tilfeller vil kunne være tilgjengelig gjennom hele etterforskningen av komplekse saker og i mange tilfeller gjennom behandling i tingrett og lagmannsrett.

Politidirektoratet antar at det bør foretas en avveining av behov for lagringstid av hensyn til kriminalitetsbekjempelse opp mot personvern hensyn og hensynet til kostnader ved lagring av data over en lengre tidsperiode. Dette kan medføre at man legger seg på en lagringstid som er kortere enn to år. Uttalelsene fra politidistriktene tilsier imidlertid at lagringstiden bør være *minst* 1 år, og at det kan være hensiktsmessig å legge seg på samme nivå som våre naboland Danmark og Finland.

Haugaland og Sunnhordaland politidistrikt uttaler:

HSPD mener som utgangspunkt at politiet må gis mulighet til benytte det handlingsrom som direktivet angir, dvs en lengst mulig lagringstid. På den annen side vil det være en fordel å harmonisere regelverket med våre naboland. Dette for å hindre at mobile kriminelle grupper flytter sin virksomhet til land som for dem har de gunstigste "rammevilkårene". De fleste land som har implementert direktivet, inkludert Danmark og Finland, har innført en lagringstid på ett år. Det advares på denne bakgrunn mot en kortere lagringstid enn ett år.

Follo politidistrikt uttaler i samme retning:

Follo politidistrikt mener personvern hensynene kan ivaretas selv med en lengde på 2 år, men ser at det kan være hensiktsmessig å legge seg på samme nivå (1 år) som de medlemslandene som allerede har implementert direktivet. Under enhver omstendighet advares det mot kortere lagringstid enn det de andre landene har innført. Kortere lagringstid her til lands kan oppfattes som et mildere regime for kriminelle, slik at de velger å begå kriminalitet her fremfor i den andre EU-landene som har innført eller er i ferd med å innføre 1 års lagringstid.

Også Romerike politidistrikt foreslår en lagringstid på minimum ett år, og uttaler:

Dagens kriminalitetsbilde med en mer organisert kriminalitet, kriminelle nettverk, tilreisende kriminelle m.m. tilsier at kriminalitet vil berøre innbyggerne i Norge mer i fremtiden enn det gjør i dag. Politiets etterforskning av disse sakene blir også vanskeligere og mer langvarig. Erfaringer fra etterforskning ved Romerike politidistrikt tilsier at teledata etter lagringsdirektivet bør lagres i minst ett år.

På bakgrunn av det ovenstående foreslår Politidirektoratet at det innføres en lagringstid på ett år.

3.3. Materielle og prosessuelle vilkår for politiets uthenting av data fra tilbyder

3.3.1 Innledning

Når det gjelder politiets tilgang til å hente ut data som er lagret foreslår departementene en skjerpelse i forhold til gjeldende rett.

For det første er det foreslått at utlevering av data bare bør kunne pålegges dersom det straffbare forholdet har en strafferamme på fengsel i 3 år eller mer. Hovedregelen i dag er at retten kan pålegge besitteren å utlevere ting som antas som bevis i en straffesak, jf straffeprosessloven § 210. Dagens bestemmelse krever ikke at det straffbare forholdet er av en viss alvorlighet.

For det andre er det foreslått at kun retten skal kunne pålegge besitteren å utlevere data. Etter gjeldende rett kan utlevering også besluttes av påtalemyndigheten etter straffeprosessloven § 205 første ledd første punktum.

For det tredje er det foreslått innføring av krav om at politiet må godtgjøre at "noen med skjellig grunn mistenkes". I dag er det tilstrekkelig for beslag og utleveringspålegg etter straffeprosessloven kapittel 16 at dataene "antas å ha betydning som bevis".

Tilbyder har lagret kunders trafikkdata i en årrekke. Politiet har i lang tid hatt anledning til å innhente trafikkdata. Politiets bruk av slike data under etterforskning, redningsoperasjoner m.v. har så vidt vites ikke vært kritisert for at metoden har vært benyttet i større grad enn loven har gitt adgang til. Det er heller ikke noe i kriminalitetsutviklingen som tilsier at politiets muligheter for å avdekke kriminalitet bør begrenses.

Metodekontrollutvalget uttaler (NOU 2009:15 side 22): "Utvalgets undersøkelser viser at politiet forholdsvis ofte innhenter opplysninger om teletrafikk (trafikkdata) som ledd i etterforskning, og at slike data må antas å ha betydning i minimum 40 prosent av sakene de innhentes i. I lys av at innhenting av slike data etter utvalgets vurdering utgjør et langt mindre inngrep i mistenktes og andres personvern enn kommunikasjonsavlytting, er dette etter utvalgets oppfatning tilfredsstillende". Slik innhenting er i flere underrettsavgjørelser karakterisert som lite inngripende sammenholdt med andre straffeprosessuelle tvangsmidler som beslag, ransaking, avlytting og – kanskje mest inngripende av alle – pågrep og varetektfengsling. Datalagringsdirektivet medfører i praksis en videreføring av (går)s dagens situasjon – i tillegg til de utvidelser som ligger i direktivet – for å sikre politiet tilgang på potensielle bevis i konkrete saker.

Politidirektoratet stiller derfor spørsmål om det er behov for å innføre skjerpelser i forhold til gjeldende rett, men har utover dette ingen grunnleggende innvendinger mot forslagene.

3.3.2 Kravet om at handlingen skal kunne medføre fengsel i 3 år eller mer.

Kravet om at utlevering av trafikkdata skal begrenses til saker med strafferammen på fengsel i tre år eller mer kan synes mindre hensiktsmessig. Søndre Buskerud politidistrikt påpeker at konkret vil det lett kunne tenkes handlinger som i realiteten fremstår som alvorlige selv om strafferammen er under tre år. Det kan for eksempel tenkes at gjentatte straffbare handlinger hvor strafferammen er lav, men som samlet sett fremstår som mer alvorlig.

Follo politidistrikt uttaler at de er av den oppfatning at 3-års grensen er for høy, og påpeker at blant annet legemsfornærmelse med skadefølge faller utenfor. Dette kan slå uheldig ut i forhold til etterforskningen av voldssaker som for øvrig er særlig prioriterte.

Dagens bestemmelser om beslag krever ikke at den straffbare handlingen er av en viss grovhet. Det foreslåtte kravet er således en skjerpelse i forhold til gjeldene rett. Som Follo politidistrikt påpeker, kan det virke inkonsekvent med et så strengt inngangsvilkår når en ellers i straffeprosessen for eksempel opererer med "fengsel i 6 måneder" for pågrep og varetektsfengsling (strpl § 171), eller "frihetsstraff" for ransaking av person, bopel m.v. (strpl § 192).

Politidirektoratet slutter seg til Søndre Buskerud politidistrikt som uttaler at begrensningen må ligge i en betraktning om at trafikkdata er nødvendig sett i forhold til den etterforskning som skal utføres og vurdert ut fra en forholdsmessighetsvurdering, jfr. strpl. § 170a.

3.3.3 Oppregningen av lovbrudd som er foreslått som alternativer til det generelle kravet om at handlingen skal kunne medføre fengsel i 3 år eller mer.

I høringsnotatet forelås å konkret angi straffbare forhold (særlige saker) med strafferamme under tre år hvor utlevering av data vil kunne skje. En slik oppregning vil muligens la seg gjøre, men det krever en større gjennomgang av hvilke lovbestemmelser, både i straffeloven og i spesiallovgivningen, som vil være aktuelle å medta.

Politidistriktene har gitt tilbakemelding på enkelte straffebud som bør være med i oppregningen, herunder nevnes:

Søndre Buskerud politidistrikt foreslår å innta straffeloven §§ 227, 1 straffealternativ, § 219, § 222, 1.ledd, 1.straffealternativ, § 200 1. og 2. ledd, § 201, § 216 og § 342, Asker og Bærum foreslår å innta straffeloven §§ 127 og 162 b, Nord-Trøndelag politidistrikt foreslår straffeloven § 390a mens Haugaland og Sunnhordaland politidistrikt foreslår å tilføye straffeloven § 201, bokstav c på listen over hvilke straffebud som uavhengig av strafferamme hjemler utlevering av trafikkdata.

Oslo politidistrikt fremhever at dagens praksis tilfredsstiller direktivets forutsetning om at det ikke skal gjelde i alle saker. Det blir også i dag foretatt en konkret vurdering i den enkelte sak, slik at det kun innhentes i saker hvor det er et særlig behov. Den enkelte sak hvor teledata begjæres utlevert må således, ut i fra behovet og den konkrete vurderingen, også karakteriseres som "særlig". Asker og Bærum politidistrikt uttaler at innhenting av trafikkdata er et kostnadsspørsmål og at de derfor vurderer nøye hvilke saker de mener det er behov for å innhente data i. Telemark politidistrikt uttaler i samme retning at bearbeiding av de innhentede data er en krevende prosess, noe som tilsier at politiet ikke har ressurser til å innhente og bearbeide data som ikke er av avgjørende betydning for etterforskningen av alvorlig kriminalitet

Oslo politidistrikt uttaler videre følgende:

Det er foreslått at en istedenfor et generelt krav om at handlingen skal kunne medføre fengsel i tre år eller mer, skal ha en oppregning av aktuelle straffebud. Oslo politidistrikt er av den klare oppfatning at hensynet til personvern er tilstrekkelig ivarettatt slik grunnvilkåret er i dag. Det skal også bemerkes at det ikke er satt slike vilkår ved vitneforklaring til retten, jf strpl. § 116. Politiet kan altså få samme informasjon fra en ansatt hos teleleverandøren, som evt må medta dokumentasjon til støtte for hukommelsen uten at det er krav om tre års strafferamme. Det bør derfor ikke stilles for strenge krav til utlevering av teledata.

Ved etterforskning av alvorlig kriminalitet, vil det i visse tilfeller være nødvendig å etterforske andre mindre alvorlige straffbare forhold opp i mot et miljø eller person for å bygge opp en sak. I en slik informasjonsinnhentingsfase vil trafikkdata være en viktig kilde. Informasjonen vil erfaringsvis gi skjellig grunn til mistanke opp i mot den kriminalitet som politiet mistenker miljøet for å bedrive. Til dette kommer at nettopp innhenting av teledata under etterforskningen av en ordinær straffesak, fører til at man avdekker at kriminaliteten er grov.

En vil også miste muligheten til å innhente trafikkdata i saker som vi i dag ikke kan tenke oss som "særlige", men som kan vesentlig endre karakter. Det kan også tenkes kriminalitetstyper som vi i dag ikke er plaget av, men som kan oppstå i stor omfang.

Det kan være vanskelig å skulle utarbeide en uttømmende oppregning av hvilke lovbud som skal omfattes. I likhet med Salten politidistrikt, ser direktoratet at det hadde vært ønskelig om domstolen hadde kunnet gjøre en skjønnsmessig vurdering av andre saker som kan være særlig vanskelig å etterforske uten å kunne benytte data. Dette vil medføre at systemet får en sikkerhetsventil.

3.3.4 Vilkåret om skjellig grunn til mistanke

Samtlige politidistrikt som har uttalt seg om dette spørsmålet, går i mot å innføre et vilkår om skjellig grunn til mistanke mot *en bestemt person*. Et slikt krav vil medføre at politiet ikke kan innhente trafikkdata i saker med ukjent gjerningsmann, eksempelvis drap og overfallsvoldtekter. I mange alvorlige saker foreligger det skjellig grunn til mistanke om en straffbar handling, men ikke til en bestemt person. I saker der gjerningspersonen er ukjent, kan trafikkdata være viktig for nettopp å identifisere hvem som står bak det straffbare forhold. Dette påpekes av flere politidistrikt, vi viser her til Gudbrandsdal og Oslo politidistrikt:

Gudbrandsdal politidistrikt:

Vi stiller oss spesielt undrende til høringsnotatets vilkår om at noen med skjellig grunn må kunne mistenkes for et straffbart forhold for at man skal få tilgang til trafikkdata, og hvor lite dette er problematisert. Hvis dette innføres, vil man ikke lengre kunne innhente stedsspesifikke trafikkdata når det har skjedd en straffbar handling med ukjent gjerningsmann for eksempel drap eller grovt ran. Dette vil medføre at det blir betraktelig vanskeligere å oppklare den mest alvorlige kriminaliteten med ukjent gjerningsmann.

Vi ser det som spesielt viktig at dette kravet ikke stilles. Ved at det neppe kan sies å være særlig inngripende for den enkelte borger at politiet får tilgang til trafikkdata som viser at telefonen hans har vært i et bestemt område til en bestemt tid, bør det være tilstrekkelig at dataene "antas å ha betydning som bevis".

Oslo politidistrikt uttaler i samme retning:

Et krav om at "noen med skjellig grunn mistenkes", vil frata politiet muligheten til å innhente avgjørende bevis/trafikkdata i svært mange saker. I et stort antall saker som etterforskes ved spesialavsnittene - alvorlig kriminalitet - foreligger det skjellig grunn til mistanke om en straffbar handling, men ikke til en bestemt person. Vi nøyer oss her med å vise til drap, overfallsvoldtekter og annen grov moduskriminalitet begått over tid, hvor teledata vil være svært viktig for å lokalisere tidspunkt for vitner/impliserte, hvem som har vært i det aktuelle området osv.

Asker og Bærum legger til at det kan være aktuelt å innhente trafikkdata i andre situasjoner enn fra mistenktes telefon. Asker og Bærum politidistrikt uttaler:

For øvrig kan en tenke seg at det i alvorlige saker kan være behov for innhenting av trafikkdata fra fornærmedes telefon/internettaksess. Det kan for eksempel dreie seg om alvorlig vold/ drap uten kjent gjerningsmann hvor opplysninger fra fornærmedes telefon/pc vil gi viktig informasjon som kan lede fram til en eventuell gjerningsmann. I slike tilfeller vil det være uheldig om det var et vilkår om at det måtte foreligge skjellig grunn til mistanke mot en bestemt person.

Troms politidistrikt anbefaler at lovgiver opprettholder dagens krav til skjellig grunn og at begrensningen for politiet knytter seg til å overbevise domstolen om at tvangsmidlet vil være av vesentlig betydning for etterforskningen. Politidistriktet uttaler:

Politimesteren er imidlertid sterkt uenig i departementets forslag hvor det kreves at noen konkret person med skjellig grunn kan mistenkes, jf høringsbrevet side 48/49.

Forslaget vil i tilfelle innebære en vesentlig begrensning i adgangen til å innhente trafikkdata i saker hvor dette erfaringsmessig har stor betydning.

Det må være tilstrekkelig som dagens regelverk rundt beslag og utleveringspålegg, at det foreligger skjellig grunn til mistanke om en straffbar handling og dataene "antas ha betydning som bevis".

Til illustrasjon vil forslag bety følgende i saker hvor ingen konkret person kan mistenkes:

- Ved etterforskning av grove seksuelle overgrep over internet vil politiet ofte kunne sitte med en eller flere IP-adresser som sentralt bevis. Datatrafikken fra denne adressen vil i tilfelle ikke kunne innhentes.
- På åstedet for et drap/voldtekt finner politiet en mobiltelefon med ukjent/uregistrert eier. Utover det politiet finner på selve mobilen vil politiet ikke kunne hente informasjon fra basestasjoner (bevegelsene i forkant) eller trafikkdata.
- En bensinstasjon på et relativt øde sted ranes midt på natten. Innhenting av basestasjonstrafikk i område vil ikke være mulig.

Politidirektoratet slutter seg til uttalelsen fra Troms politidistrikt. Vi anser at det må være tilstrekkelig som dagens regelverk rundt beslag og utleveringspålegg at det foreligger skjellig grunn til mistanke om en straffbar handling og at dataene "antas ha betydning som bevis".

3.3.5 Formell kompetanse - Retten

Etter gjeldende rett har påtalemyndigheten kompetanse til å beslutte beslag, men spørsmålet om beslaget skal opprettholdes kan kreves brakt inn for retten. Politidirektoratet mener at dagens ordning bør opprettholdes, og at det ikke anses nødvendig å oppstille et krav om domstolsbehandling.

Vi slutter oss til Oslo politidistrikt som uttaler:

Kompetansen til å begjære teledata utlevert bør ligge hos påtalemyndigheten, som er den nærmeste til å vurdere viktigheten av teledata i den enkelte sak. Datalagringsdirektivet stiller ingen krav til nasjonal lovgivning på dette punktet, og en kan ikke se behovet for en begrensning av påtalemyndighetens kompetanse. Oslo politidistrikt kan ikke se at dette er nærmere begrunnet. En generell henvisning til at omfanget av innhenting av trafikkdata er stort, kan ikke tas til inntekt for at myndigheten bør legges til domstolene. Dette tilsier kun at betydningen av trafikkdata i etterforskningen er stor.

Erferingene tilsier at rettsikkerheten er ivaretatt med dagens ordning, og en overføring av ansvaret til retten vil følgelig ikke være et begrunnet bidrag til økt rettsikkerhet. Samtlige som arbeider i påtalemyndigheten har juridikum, og de personene som arbeider med organisert kriminalitet har gjennomgående også lang arbeidserfaring. Påtalemyndigheten har ansvaret for etterforskningen og at straffeprosessen blir fulgt, og en mener det kan legges til grunn at ansvaret blir gjennomført på en betryggende måte.

En overføring av myndigheten til retten, vil bidra til en vesentlig økt saksbehandling og ressursbruk hos politiet, påtalemyndigheten og tingretten. I hver enkelt sak må tingretten få oversendt påtegning med begrunnelse for begjæringen og kopi av samtlige saksdokumenter – pr. i dag er dette omlag 1900 saker årlig. Dette vil være en unødvendig tapping av politiets og tingrettens ressurser, uten at det vil være et begrunnet bidrag til økt rettssikkerhet.

Dersom det innføres et krav om at trafikkdata kun kan utleveres etter beslutning fra retten, stiller vi spørsmål ved om det er gjennomtenkt at påtalemyndigheten ikke gis hastekompetanse. Vi viser til at påtalemyndigheten er gitt hastekompetanse i tvangsmidler som er langt mer inngripende, eksempelvis kommunikasjonsavlytting og romavlytting hvor politimesteren er tillagt hastekompetanse, jf strpl § 216d.

3.4 Andre myndigheters tilgang til data

Dette spørsmålet reiser etter vårt syn en prinsipielt viktig problemstilling. Formålet med direktivet er å bekjempe kriminalitet og dette er en oppgave for politi og påtalemyndighet. Politidirektoratet, i likhet med Nord-Trøndelag politidistrikt, ser dette som et viktig prinsipp som ikke må uthules ved at man gir andre tilsynsorganer tilgang til data på samme måte som for politi og påtalemyndighet.

Det fremkommer av høringsnotatet at Kredittilsynet har tilgang til trafikkdata i dag. Dersom Kredittilsynet fortsatt skal ha tilgang til trafikkdata, bør de undergis de samme vilkår for tilegnelsen som politiet. Dersom det innføres krav om domstolsbehandling for politiets tilgang til trafikkdata, bør samme krav gjelde for Kredittilsynets tilgang.

4 Lagring av data – sikkerhet, lagringssted m.v

4.1 Sikkerhet

Politidirektoratet forutsetter at det ikke er politiet som skal foreta lagring av data. Verken politi eller teletilbyder skal ha fri adgang til informasjonen. Politiets tilgang skal skje som ledd i etterforskning av straffbare forhold. Hos tilbyder må det legges vekt på informasjonssikkerhet og internkontroll. Kun særlig autorisert personell skal ha tilgang, og informasjonen bør lagres kryptert, eller i ikke-lesbare rådata. Verken politi eller tilbyder skal ha tilgang til eller innsyn i dataene uten at det foreligger hjemmel for dette.

4.2 Lagring hos den enkelte tilbyder eller i sentral database

I høringsnotatet fremkommer det at departementene har utredet en løsning for lagring av data i en sentral database, men at det etter en avveining av flere hensyn, ikke foreslås å etablere en sentral lagringsløsning. Politidirektoratet vil bemerke at en sentral lagring vil være en god løsning. En sentralisering av lagringen vil medføre at tilbyderne har lik praksis slik at man lettere kan garantere for at hensyn til lovgivning, regler og personvern blir godt ivaretatt. Videre vil vi anta at en slik løsning vil være mer kostnadseffektiv både for tilbyderen og for myndighetene, samtidig som det vil lette den praktiske uthenting av trafikkdata for politiet.

5 Økonomiske og administrative konsekvenser

5.1 Kostnadsfordeling

Dagens kostnadsmodell i Norge når det gjelder lovbestemt tilgang til informasjon, er en delingsmodell hvor ekomtilbyderne har en tilretteleggingsplikt og forutsettes å dekke kostnadene knyttet til denne plikten. Tilbydernes driftskostnader/uthentingskostnader

dekkes av politiet i henhold til avtaler. Dette følger av lov 4. juli 2003 nr. 83 om elektronisk kommunikasjon (ekomloven) § 2-8. Høringsnotatet foreslår å videreføre dagens kostnadsfordeling.

Politidirektoratet vil bemerke at dagens løsning innebærer betydelige utfordringer, og *ikke* bør videreføres. I de senere årene har det vært gjentatte drøftelser mellom Politidirektoratet på den ene siden og tilbyderne på den annen side om hvilke kostnader som skal dekkes av tilbyderne og hvilke kostnader politiet skal dekke etter ekomloven § 2-8. Loven oppstiller et skille mellom investeringskostnader som tilbyder skal betale og driftskostnader som politiet skal betale, men verken lovtekst eller forarbeider til ekomloven omhandler spørsmålet om sontringen mellom drifts- og investeringskostnader. Det hefter således en betydelig usikkerhet rundt plasseringen av de vesentligste kostnadene, som omfangsmessig har økt i sterk grad i de senere år. I dagens marked med et stort antall tilbydere, er problemstillingen av stor betydning. Skulle staten ved politiet måtte bære betydelige kostnader for hver enkelt tilbyder, i et marked i sterk vekst, ville dette medføre en kostnadseksplasjon som ikke har noen som helst sammenheng med en eventuell økning i antall henvendelser fra politiet. Vi vil også bemerke at politiets påvirkningsmuligheter på kostnadssiden vil være meget begrenset grunnet manglende nærhet til de kostnadsgenererende tjenester. Dagens løsning som forutsetter individuelle forhandlinger og avtaleinngåelse mellom Politidirektoratet og hver enkelt tilbyder er svært ressurskrevende for begge parter. Politidirektoratet har på midlertidig basis inngått avtaler om priser med enkelte tilbydere. For alle de øvrige tilbyderne er spørsmålet om pris pr i dag uavklart.

Vi vil stille spørsmål ved om det er riktig at politiet helt eller delvis skal dekke tilbyderne kostnader ved å etterkomme offentligrettslige pålegg for å bekjempe kriminalitet. På andre områder hvor myndighetene innfører offentligrettslige krav og plikter blir kostnadene belastet den enkelte aktør. Vi viser eksempelvis til hvitvaskingsregelverket som pålegger finansinstitusjoner, advokater, revisorer og andre rapporteringspliktige store investerings- og driftskostnader uten at dette medfører annet enn milde protester fra disse bransjene. Hovedinnvendingen fra finansbransjen har vært at offentlige etater som for eksempel skatte- og tollvesenet ikke pålegges de samme pliktene. Pliktene etter hvitvaskingsregelverket omfatter blant annet innsamling og lagring av data om kunden (kundekontroll), utredning av mistenkelige transaksjoner med henblikk på å avkrefte mistanken, samt rapportering til myndighetene, herunder oversendelse av betydelig dokumentasjon som kontoutskrifter, kontrakter og lignende. Rapporteringspliktige etter hvitvaskingsregelverket bærer alle kostnadene forbundet med dette selv. Finansnæringen synes i økende grad å ta et samfunnsansvar for kriminalitetsbekjempelse. Politidirektoratet vil bemerke at også tilbyderne av ekomnett- og tjenester har et samfunnsansvar på lik linje med Finansnæringen.

Refusjonsregelen i ekomloven § 2-8 andre ledd først ble foreslått under samferdselskomiteens behandling av ekomloven. Bestemmelsen var ikke inntatt i proposisjonen, og ordlyden i lovutkastet sa således ikke noe om kostnadsfordelingen. Dette kan tyde på at bestemmelsen konsekvensmessig er lite gjennomtenkt.

Med utgangspunktet i at dagens løsning har store svakheter og lovgrunnlaget inneholder betydelige uklarheter, mener Politidirektoratet at dagens regulering av tilretteleggingsplikten må endres.

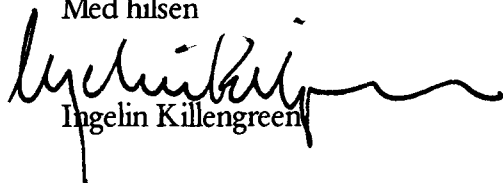
Politidirektoratet foreslår at man velger en løsning som i Danmark, hvor tilbyderne må dekke merkostnader som følge av lagringsplikten selv, mens politiet betaler for uthenting. Vi foreslår videre at myndighetene i forskrift fastsetter hva pris per uthenting skal være. Både tilbyderne og politiet unngår med en slik løsning ressursbruk med å fremforhandle avtaler. Vi mener at en slik løsning vil sikre den beste og mest kostnadseffektive løsning for samfunnet. Dersom dagens kostnadsmodell skal videreføres, vil det være behov for – fortrinnsvis i forskrift - å klargjøre nærmere hva som er å anse som investeringskostnad og hva som er driftskostnad.

5.2 Statistikk

Det følger av høringsnotatet at ved en implementering av datalagringsdirektivet i norsk rett er norske myndigheter forpliktet til årlig å sende inn statistikk til ESA om datalagringen. Det skal føres statistikk om antall saker hvor anmodningen blir imøtekommet, tiden mellom lagringstidspunkt (dato) og etterspørsel etter data og saker der anmodning om data ikke har blitt imøtekommet. Departementene foreslår at det er politiet og andre myndigheter som anmoder om data som må føre statistikken og videre sende denne til Post- og teletilsynet for oversendelse til ESA.

Politidirektoratet bemerker at, for det tilfelle at det er politiet som skal føre statistikken, vil dette medføre økt bruk av ressurser.

Med hilsen



Ingelin Killengreen

VEDLEGG



POLITIET

MOTTATT
22 MAR 2010

POLITIDIREKTORATET	
22 MARS 2010 5	
Arkiv A08-13	Prosjekt 008
Saksnr. 2010/00134	Polis 006

Politidirektoratet
Postboks 8051 Dep.
0031 OSLO

Deres referanse
201000134 -2 008

Vår referanse
2010/00933-2 500

Dato
19.03.2010

Høring om datalagring

Det vises til Deres brev av 22.02.2010.

For Romerike politidistrikt sin del er det kun knyttet kommentarer til de delene av høringsnotatet der politidistriktet mener vi kan supplere eller bidra med noe utover det som allerede fremkommer i høringsnotatet og vedleggene.

Omfang

Romerike politidistrikt har ingen registrering av antall saker der trafikkdata og lokaliseringsdata er benyttet. Beskrivelse av anvendelse av trafikkdata/lokaliseringsdata for bruk i etterforskningen bygger derfor på erfaringer fra trafikkdata knutepunktet i distriktet, samtale med utvalgte etterforskere, eksempler fra kjente saker etterforsket på Romerike.

Alt tilsier at trafikkdata er en meget anvendt bevisinnhenting i større straffesaker i Romerike politidistrikt. Spesielt gjelder dette saker som f.eks. etterforskning av drap med ukjent gjerningsmann, ran med ukjent gjerningsmann, seksuelle overgrepssaker, trusler, grove tyverier der etterforskningen tilsier at disse er organiserte, grove narkotikaforbrytelser m.m.

Omfanget er størst når det gjelder trafikkdata for GSM nettet. Grunnen til dette er først og fremst at dette frem til i dag har vært den mest anvendte måten å kommunisere på mellom de kriminelle. Det faktum at politiet gjennom tid har opparbeidet seg bedre kompetanse på bearbeidelse av slike teledata fremfor IP basert kommunikasjon på e-post og web spiller også helt klart inn.

Tendensen er trolig at bruk av innhentede data fra internettaksess og e-post vil få en økende betydning for etterforskningen av straffesaker i tiden fremover. Dette gjør seg spesielt gjeldende da denne måten å kommunisere på gjøres mer mobil ved utbygging av nye landsdekkende mobile bredbåndsnett og tilgang til håndholdte enheter som for bredbåndskommunikasjon.

Romerike politidistrikt

Anvendelse i etterforskningen

Politiets etterforskning generelt kan beskrives i to kategorier, proaktiv etterforskning og reaktiv etterforskning, der de fleste etterforskningene er reaktive. Det medfører i praksis at den straffbare handlingen allerede er begått og at politiet må tilbake i tid for å sikre beviser knyttet til den straffbare handlingen og eventuelle gjerningsmenn.

Dagens kriminalitetsbilde viser at flere typer kriminalitet blir mer og mer organisert. Dette sett i relasjon til det faktum at de fleste personer i dag bærer med seg en mobiltelefon, gjør trafikkdata til et svært relevant, og i flere tilfeller avgjørende bevis i straffesaker etterforsket på Romerike.

Selve kommunikasjonen mellom de forskjellige aktørene i en straffbar handling kan i mange tilfeller også sies å være avgjørende for at selve gjennomføringen skal lykkes.

Eksempler på nytteverdi

I flere alvorlige straffesaker etterforsket ved Romerike politidistrikt er det avdekket at bevisene for det straffbare forholdet i seg selv ligger i opplysninger fra trafikkdata.

Organiserte kriminelle forsøker å skape avstand i tid og sted mellom seg selv og den straffbare handlingen. Kontakten mellom bakmannen og personen som utøver selve handlingen hadde således ikke latt seg bevisføre uten tilgang til trafikkdata.

I andre saker har politiets tilgang til trafikkdata gjort politiet i stand til å gå tilbake i tid og rekonstruere kontakten gjerningsmennene har hatt med hverandre (personspesifikke spor) samt dokumentere hvilke basestasjoner de har vært tilknyttet (stedsspesifikke spor), ofte i strid med deres egne forklaringer.

Romerike politidistrikt har benyttet trafikkdata som avgjørende bevis i flere straffesaker fra midten på 90-tallet og frem til dags dato.

Eksempler på saker der trafikkdata har vært avgjørende for etterforskningen i Romerike politidistrikt:

1. City-ranet Lillestrøm, 1998. Flere ranere bevæpnet med skarpladde militærvåpen tok seg inn på handlesenter i Lillestrøm på natten. Senere overfalt de og ranet 2 vektere fra et vaktelskap som var kommet til stedet for å hente dagens omsetning. Ranet bar preg av planlegging og brutalitet. Innhenting av trafikkdata fra basestasjoner gjorde at politiet kunne knytte flere mellommenn til ranet. Senere etterforskning og innhenting av trafikkdata på disse personene gjorde politiet i stand til å pågripe gjerningsmennene. Hovedpersonene ble dømt til henholdsvis 8 og 9 års fengsel. Uten innhenting av trafikkdata på basestasjonen ville politiets etterforskere ikke hatt muligheter til å avdekke gjerningsmennene.
2. Drosjedrapet i Nittedal i 1999. Utskrifter fra fornærmedes telefon dokumenterte kontakt med mistenkte i tiden rett forut for selve drapet. Deretter innhentede trafikkdata fra mistenktes telefon knytter ham direkte til handlingen og impliserer ytterligere en person. Begge de to blir dømt i saken. Etterforskeren i saken mener de innhentede trafikkdata var helt avgjørende for bevisføringen og at man ikke hadde

funnet frem til gjerningsmennene uten trafikkdata.

3. Innførsel og omsetning av flere kilo heroin 1999 - 2000. Gjennom spaning og kommunikasjonskontroll avdekker politiet innførsel av 5 kilo heroin knyttet til et utenlandsk nettverk, tilreisende utlendinger midlertidig bosatt på Romerike og et pakistansk nettverk på Romerike. Trafikkdata bakover i tid avdekker ennå 2 innførsler av heroin der modus, kontaktmønster og reiser er lik den avdekkede innførselen. Bevisene fra trafikkdata viser hovedmennenes roller over tid og medfører domfellelse av hovedmenn, kurer og mottagere i Norge. Hovedmennene får 15 og 16 års ubetinget fengsel. Rolleforståelse, organisering og handlingsmønster over tid hadde ikke blitt avdekket uten trafikkdata.
4. Funn av til sammen 28 kilo amfetamin i Fetsund 2004. Lensmannen i Fet og Rælingen på Romerike rykker ut til en gård der det er meldt om skyting. Stedet er forlatt. På stedet finner han 28 kilo amfetamin i en fryseboks. På stedet finner man en rekke mobiltelefoner og SIM-kort. Ingen av disse er registrert på personer. Avhør av vitner og annen etterforskning avdekker 2 aktuelle personer til huset der narkotikaen blir funnet. Begge er godt kjent av politiet for grov narkotikakriminalitet fra tidligere. Ved innhenting av trafikkdata klarer politiet å binde 3 helt andre personer til partiet med narkotika. Lagrede tekstmeldinger på beslaglagte telefoner avdekker handlingene. Sammenholdte trafikkdata mellom gjerningsmennenes registrerte åpne telefoner og telefonene funnet på gården knyttet de mistenkte til disse telefonene og avdekker ytterligere innførsel og omsetning av til sammen 250 kilo hasj og 40 kilo med amfetamin. Hovedmannen blir dømt til 15 års fengsel. Innhentede trafikkdata var helt avgjørende som bevis i saken. De innhentede trafikkdataene viste videre at de 2 personene som først var siktet i saken kun hadde en svært perifer rolle.
5. Etterforskning av multi-kriminelt nettverk, Romerike politidistrikt 2006 – 2007. Saken hadde utgangspunkt i en analyse av flere saker der det forelå trafikkdata. Gjennom analysen avdekket politiet et miljø man mente forsynte flere personer og flere nettverk med narkotika, og andre straffbare handlinger. Gjennom den videre etterforskningen beslaglegger Romerike politidistrikt i samarbeid med flere distrikter store partier med narkotika, bl.a. 15 kilo heroin, 40 kilo amfetamin, 50 kilo amfetamin, 100 kilo hasj, 2 kilo amfetamin, 2 kilo amfetamin, 2 kilo kokain samt en rekke mindre beslag. I tillegg avdekker etterforskningen omsetning av flere kilo heroin i nettverket. Underveis i etterforskningen har politiet innhentet ca 100 utskrifter av teletrafikk. Opplysninger fra teletrafikken har gjort politiet i stand til å avdekke hvordan hovedmennene har kommunisert med hverandre. Opplysninger fra teledata sammenholdt med annen etterforskning var avgjørende bevis i flere av hovedforhandlingene i retten.

Rettsikkerhet

Oppsummeringsmessig for eksemplene bør det nevnes at Romerike politidistrikt også under etterforskning av flere større saker har fått kritikk fra de tiltalte i saken gjennom deres forsvarere, for manglende innhenting av trafikkdata i de tilfeller det ikke er gjort.

Det må ut fra dette også være slik at innhenting av trafikkdata i større mer alvorlige saker i flere tilfeller forventes av tiltalte selv og deres forsvarer. Man ønsker gjennom dette å kontrollere politiets etterforskning for øvrig.

Manglende innhentede trafikkdata blir av de tiltalte og deres forsvarere i visse tilfeller anført som en svekkelse av politiets etterforskning og begrensende for deres mulighet til å føre sitt forsvar.

Hva skal lagres

IMEI/IMSI identer for B og C nummer

Forslaget i høringsnotatet vil generelt gi adgang til flere opplysninger enn det man får tilgang til gjennom dagens utskrifter. Opplysninger det siktes til er IMEI/IMSI identer for B og C nummer samt lokaliseringinformasjon ved avslutning av samtalen.

Denne informasjonen vil klart være relevant for politiets etterforskning. Innformasjon om IMEI/IMSI identer for B og C nummer kan man etter dagens system få tilgang til gjennom å be om trafikkdata for disse numrene der dette er relevant. Dette er også i dag ofte tilfelle. I det dagens utskrifter mangler denne informasjonen, innhentes ofte supplerende data gjennom tilleggsutskrifter, ofte kombinert med IMEI søk der dette er relevant for etterforskningen. Ved slik innhenting av trafikkdata vil man også oftere få tilgang til urelevante data for saken. Mer komplett informasjon knyttet til primære data slik som det er foreslått i lagringsdirektivet på side 29 og 30 vil derfor heller ha som potensial å begrense omfanget av data som blir utlevert til Politiet enn dagens ordning.

Mislykkede opprigninger

Dagens ordning gir ikke politiet opplysninger om mislykkede opprigninger. Dette er foreslått som en del av lagringsdirektivet. Informasjon fra en mislykket oppringing vil i praksis gi informasjon om grunnlaget for samtaler som følger etter – hvem var det som initierte samtalen. Videre vil gjentatte opprigningsforsøk over tid si noe om behovet for kommunikasjon.

Lagring i sentral database

I høringsnotatet fremkommer det at departementene har utredet en løsning for lagring av data i sentral database. Det fremheves noen praktiske grunner for at dette er en god løsning.

Med dagens løsning har politidistriktene forskjellige rutiner.

Politidistriktene forholder seg til flere forskjellige teletilbydere. Teletilbyderne har ikke lik praksis i forhold til politiet. I tillegg har flere av tilbyderne over tid forandret rutinene sine.

Sentralisering av lagringen ville medført at man hadde lik praksis og at man lettere kunne garantere for at hensyn til lovgivning, regler og personvern ble godt ivaretatt. Slik sentral lagring burde etter Romerike politidistrikt sin mening utredes sammen med ett sentralt kontaktpunkt i politiet.

Lagringstiden

I høringsnotatet er det gjennom drøftelser kommet frem til en lagringstid på 6 måneder. Man peker på at dette er lengre enn det dataene lagres i dag, henholdsvis 3 og 5 måneder.

I drøftelsene er det lagt vekt på argumenter om at politiet oppklarer saker som f. eks. Nokas-saken m.m. selv med en kortere lagringstid.

I drøftingen tas det ikke høyde for at det i dag er en rekke saker politiet ikke oppklarer. Sentrale myndigheter i Norge er generelt bekymret for politiets lave oppklaring av saker.

I tillegg til dette er det gjennom flere år ved Romerike politidistrikt vært slik at politiet gjennom de kriminelle miljøene og gjennom lengre etterforskninger får opplysninger om gjerningsmenn som står bak alvorlig kriminalitet tilbake i tid. Trafikkdata tilbake i tid i slike saker har vist at dette ofte kan resultere i oppklaring. Disse sakene etterforskes i dag ikke og synes ingen andre steder enn i politiets dårlige oppklaringsprosent.

Argumentet er faren for et dårligere personvern og "den nedkjølende effekten datalagring har på borgernes vilje til åpen fra kommunikasjon".

Argumentasjonen er med andre ord slik at hvis man lagrer samtaledata i 1 år knyttet til person A, kontra det å lagre samtaledata for person A i 6 måneder, så vil den lovlige borgeren A være skeptisk over å kommunisere med slekt og venner og personvernet rundt person A står i større fare.

Argumentasjonen i denne sammenhengen der man som en ramme for datalagring ser for seg strenge krav for lagring, høy datasikkerhet, lovbeskyttet tilgang til dataene gjennom rettsystemet og skjellig grunn til mistanke kravet, synes langt på vei å være teoretisk og oppkonstruert.

Rent praktisk vil det være slik at det er de nyeste og ferskeste trafikkdataene som har mest potensialet for å skade noen i personvernsammenheng. Data fra forrige uke kan lett ses i sammenheng med kjente hendelser. Data som er over 6 måneder gamle vil vanskeligere kunne settes i noen relasjon av uvedkommende.

Dagens kriminalitetsbilde med en mer organisert kriminalitet, kriminelle nettverk, tilreisende kriminelle m.m. tilsier at kriminalitet vil berøre innbyggerne i Norge mer i fremtiden enn det gjør i dag. Politiets etterforskning av disse sakene blir også vanskeligere og mer langvarig.

Erfaringer fra etterforskning ved Romerike politidistrikt tilsier at teledata etter lagringsdirektivet bør lagres i minst ett år.

Med hilsen


Kari Torkelsen
visepolitimester

Saksbehandler: Politioverbetjent Werner Male



POLITIET

Politidirektoratet
Postboks 8051 - Dep
0031 OSLO

MOTTATT

18 MAR 2010

POLITIDIREKTORATET	
18 MAR 2010	
Arkiv 08-13	Arkivkode 008
Saksnr. 10/134	Dok.nr. 4

Deres referanse
2010/00134-2 008

Vår referanse
2010/00222-2 053

Dato
12.03.2010

Høring om datalagringsdirektivet

Det vises til Deres høringsbrev av 22.02.10.

Vi vil begrense høringsuttalelsen til kun å rette seg mot det som etter vårt syn er det mest sentrale med datalagringsdirektivet.

Politiets behov for tilgang til trafikkdata

Det er ingen tvil om at politiet har et stort behov for å få tilgang til trafikkdata i en hel rekke saker – både svært alvorlige og mindre alvorlige saker.

Det helt opplagte er at politiet må ha tilgang til trafikkdata når det skal etterforske saker hvor Internet er brukt i selve den straffbare handling – for eksempel ved spredning av barnepornografi over Internet.

Det er også av stor betydning å få tilgang til trafikkdata når det har skjedd en mer eller mindre alvorlig forbrytelse med ukjent gjerningsmann på et bestemt sted. I disse tilfellene kan det være av avgjørende betydning å få kartlagt hvilke personer som har vært i området i et bestemt tidsrom. Et viktig element i denne kartleggingen er å finne ut hvilken telefontrafikk det var i området i det aktuelle tidsrommet. Denne trafikken fremgår av basestasjonsutskrifter. Av disse utskriftene vil det fremgå hvilke personer som de aktuelle telefonene står registrert på.

Det er en rekke alvorlige saker, hvor denne informasjonen har vært av stor betydning for eksempel "NOKAS-saken". Her ga basestasjonsutskriftene opplysninger om vitner men også om de såkalte "ranstelefonene". Disse ga bla. informasjon om ranernes adkomst/flukt og forberedelseshandlinger.

I motsatt ende ligger den såkalte Lena-saken. Dette var en kvinne som forsvant utenfor Stavanger. Her gikk det så lang tid før politiet forsøkte å innhente trafikkdata, at dataene ble slettet før politiet kom med anmodningen. Dette medførte store vansker for

Gudbrandsdal politidistrikt

etterforskningen og var et viktig tema hele tiden – også i retten. Eks. samboeren ble domfelt til 19 års forvaring i tingretten, men dommen er anket.

I den senere tid har det også vist seg at basestasjonsutskrift er et viktig hjelpemiddel i kampen mot de omreisende vinningskriminelle. I tilfeller hvor det for eksempel begås grove tyverier fra bolig på forskjellige steder i et noenlunde sammenhengende tidsrom, har det vist seg å være av stor betydning å finne ut om man kan identifisere om noen telefoner har vært i flere av områdene hvor innbruddene har skjedd.

Det kan også være av stor betydning å kunne ta en telefonutskrift av et bestemt abonnement i saker hvor en person er anmeldt. Det kan være av avgjørende betydning å finne ut hvem han har kommunisert med til hvilken tid og på hvilket sted (basestasjon). Det samme vil også ofte gjelde hans bruk av pc i kommunikasjonssammenheng.

Type data som bør lagres

Her slutter vi oss til høringsnotatet.

Lagringstidens lengde

Det er flere sakstyper hvor en etterforskning ikke vil starte før det har gått en viss tid. Spesielt kan dette gjelde i forsvinningsaker for eksempel "Lena-saken" og ved spredning av barnepornografi. Lagringstiden bør således være av en viss lengde. Passende lengde antas å være to år.

Vilkår for at politiet skal få tilgang til trafikkdata

Vi stiller oss spesielt undrende til høringsnotatets vilkår om at noen med skjellig grunn må kunne mistenkes for et straffbart forhold for at man skal få tilgang til trafikkdata, og hvor lite dette er problematisert.

Hvis dette innføres, vil man ikke lengre kunne innhente stedsspesifikke trafikkdata når det har skjedd en straffbar handling med ukjent gjerningsmann for eksempel drap eller grovt ran. Dette vil medføre at det blir betraktelig vanskeligere å oppklare den mest alvorlige kriminaliteten med ukjent gjerningsmann.

Vi ser det som spesielt viktig at dette kravet ikke stilles.

Ved at det neppe kan sies å være særlig inngripende for den enkelte borger at politiet får tilgang til trafikkdata som viser at telefonen hans har vært i et bestemt område til en bestemt tid, bør det være tilstrekkelig at dataene "antas å ha betydning som bevis".

Formell kompetanse

I forslaget fremgår det at det er retten som skal ha kompetanse til å pålegge besitteren å gi ut data. Vi støtter at primærkompetansen legges til retten. Vi mener allikevel at det er uheldig at påtalemyndigheten ikke får en hastekompetanse.

Flere at sakene vil oppstå til tider, hvor det ikke er mulig å få en beslutning fra retten. Dette kan være særdeles alvorlige saker, hvor det virkelig haster. I slike tilfeller bør ikke politiet være henvist til å vente på rettens beslutning.

A handwritten signature in black ink, consisting of a stylized 'A' followed by a long horizontal line that ends in a small 'R' shape.

Arne Hammersmark
politimester



POLITIET

MOTTATT

29 MAR 2010

POLITIDIREKTORATET
Postboks 8051 Dep
Besøk: Hammersborggata 12
0031 OSLO

POLITIDIREKTORATET	
29 MARS 2010	
Ansvar: A 08-13	Ansvar: 008
Saksnr: 1900134	Dokument: 13

Deres referanse
2010/00134-2 008

Vår referanse
2010/00681-2 008

Dato
25.03.2010

INNSPILL KNYTTET TIL HØRINGSUTTALELSE OM DATALAGRING

Det vises til politidirektoratets brev av 22.02.2010, hvor det anmodes om innspill til høring om datalagring.

Nedenfor er det knyttet kommentarer til enkelte av de problemstillinger som er fremhevet i høringsnotatet (pkt. 1-4).

1. Presisering av hva som eventuelt skal lagres.

I datalagringsdirektivets artikkel 5 fremkommer det hvilke kategorier av data som skal lagres. På bakgrunn av at datalagringsdirektivet her kan gi rom for tolkning er det i høringsnotatet foreslått en presisering av hva som skal lagres.

Nevnte presisering fremstår som viktig, idet man da unngår at tilbydere har ulike oppfatninger av hvilke data som skal lagres.

De presiseringene som fremkommer av høringsnotatet synes å dekke de nødvendige data knyttet til de forskjellige kommunikasjonsformer.

2. Lagringstid m.v

Ved spørsmål om lagringstidens lengde er det to hensyn som står mot hverandre. På den ene side hensynet til personvernet og på den andre side ønske om å oppklare og irrettføre straffbare forhold.

Det synes som om majoriteten av de land som har implementert datalagringsdirektivet har fastsatt en lagringstid på ett år. Hensynet til en størst mulig lik praktisering av lagringstiden blant de land som har implementert lagringsdirektivet skulle derfor tilsi en tilsvarende lagringstid, dvs. på ett år.

Østfold politidistrikt

Retts- og påtaleenheten, besøk: Signat Skaldsgt. 5
Post: Postboks 73, 1701 SARPSBORG
Tlf: 69 11 33 00 Faks: 69 11 33 05
E-post: post.ostfold@politiet.no

Org. nr.: 983 996 078
Bankgiro: 7694.05.11581

I tillegg til ovennevnte skal det bemerkes at en kortere lagringstid vil kunne skape vanskeligheter ved etterforskning av enkelte sakstyper. Det vises her til straffesaker knyttet til menneskehandel, hvor offeret har en refleksjonsperiode på 6 måneder. Formålet med perioden er at offeret skal kunne bryte med miljøet bak menneskehandelen og legge til rette for at bakmenn skal kunne straffeforfølges. I etterforskning av denne type saker vil innhenting av elektroniske spor være av stor betydning. En kortere lagringstid enn ett år vil imidlertid medføre at etterforskning mot bakmenn vil bli betydelig vanskeliggjort.

Videre vises det til etterforskning av straffesaker knyttet til innførsel av narkotika. Det er ikke uvanlig at det avdekkes at kurerer tidligere har vært i Norge, og da trolig også har innført narkotika. I angjeldende tilfelle er det av stor betydning å innhente trafikkdata for å knytte mottager til innførselen. Også i denne type saker vil en kortere lagringstid enn ett år vanskeliggjøre straffeforfølging mot mottagerleddet.

Når det gjelder etterforskning mot seksuelle overgrep mot barn på internett vil også en kortere lagringstid enn ett år vanskeliggjøre straffeforfølging mot gjerningsmenn. I denne type saker vil innhenting av data være sentral for etterforskningen. En kort lagringstid vil her medføre at straffbare forhold ikke vil la seg straffeforfølge.

Lagringstiden for data bør fremstå som lik for de forskjellige teknologiene. Betydningen av de forskjellige teknologiene i etterforskningen tilsier ikke at det skal skilles på lagringstiden. En lik lagringstid vil også innebære en oversiktlig ordning, som også tar hensyn til fremtidig utvikling innenfor kommunikasjonsteknologien.

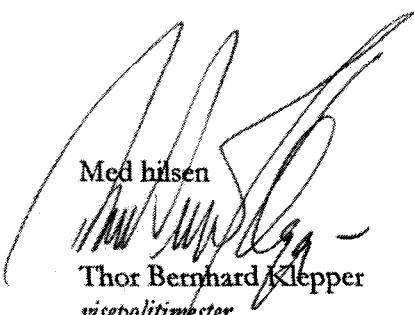
3. Oppregning av lovbrudd som er foreslått som alternativer til det generelle krav om strafferamme på 3 år.

Ved å sammenholde forslaget i høringsnotatet med erfaringer fra saker hvor det er innhentet trafikkdata, finner man at de lovbud som er beskrevet i høringsnotatet synes å dekke de relevante områder.

4. Vilkår om skjellig grunn til mistanke

Innføring av et krav om skjellig grunn til mistanke mot en bestemt person vil i stor grad begrense straffeforfølgingen i flere typer av straffesaker. Det vises her til at det i straffesaker knyttet til narkotika ikke er uvanlig at kurer har hatt kontakt med flere personer. For å få oversikt over et eventuelt mottagerapparat vil det være av betydning å innhente trafikkdata fra disse personene. Et krav om skjellig grunn til mistanke mot person vil i betydelig grad kunne hindre avdekking av et mottagerapparat.

Såfremt det skal etableres et krav om skjellig grunn til mistanke må dette ikke knyttes til bestemt person. Dette ligger nærmest dagens krav og vil i større grad muliggjøre avdekking av kriminelle nettverk og bekjempe alvorlig kriminalitet.



Med hilsen

Thor Bernhard Klepper
visepolitimester

Saksbehandler:
Politinspektør Espen
Jamissen
Tlf 69 11 92 56



POLITIET

POLITIDIREKTORATET	
31 MAR 2010	
Arkiv 08-13	Arkivkode 008
Saksnr 10/134	Dok nr 19

MOTTATT

31 MAR 2010

Politidirektoratet
Pb 8051 dep
0031 OSLO

Deres referanse
201000134

Vår referanse
2010/00643-3 008

Dato
22.03.2010

HØRING - OM DATALAGRING

Det vises til Politidirektoratet brev av 220210, og Samferdselsdepartementets høringsnotat av 080110.

Enkelte av spørsmålene viser til Samferdselsdepartementets høringssvar. I disse tilfeller har ikke politimesteren i Søndre Buskerud ytterligere kommentarer og Samferdselsdepartementets svar tiltres.

I vårt høringssvar har vi fulgt rekkefølgen i brevet fra Politidirektoratet av 220210.

Generelt (Avsnitt 3)

Det er åpenbart at politiet i forbindelse med etterforskning av straffesaker og i forberedelse til slik etterforskning må kunne nyttiggjøre seg av lagrede trafikkdata. I slike typer saker har aktørene uten unntak hatt telefonisk kontakt i forkant, under og etter at det straffbare har blitt gjennomført.

I narkotikasaker er det særlig aktuelt å vite hvem som snakker med hvem, hvor ofte dette skjer, når på døgnet det skjer, hvor de involverte befant seg, hvilke telefoner (imei) og telefonnummer som blir/ble benyttet.

Et moment er at disse opplysningene gir politiet kunnskap om hvor og når den operative innsatsen skal rettes.

Et annet moment er at politiet skal kunne bevise hvem som er de faktiske aktørene i en eventuell straffesak.

Et tredje moment er at politiet stadig får tilgang til opplysninger som gjør at vi må kunne sjekke ut om det foreligger tilstrekkelig informasjon om det kan iverksettes etterforskning. Dette gjelder særlig i saker knyttet opp mot alvorlig organisert

Søndre Buskerud politidistrikt

Politimesteren, besøk: Grønland 36
Post: Postboks 1087, 3001 Drammen
Tlf: 32 80 55 00 Faks: 32 80 59 57
E-post: post.sondre.buskerud@politiet.no

Org. nr.: 983998119
Bankgiro: 7694.05.11409

kriminalitet som sjelden blir anmeldt av tredje person, men som politiet selv må iverksette etterforskning mot.

Omfanget vedr bruken av trafikkdata og dataenes betydning for innhentingsformålet vil variere fra sak til sak, samt hvilken kompetanse som er tilgjengelig hva gjelder analyse av dataene. I noen saker vil det kun være aktuelt å etterforske mot enkeltpersoner eller et fåtall personer, og i andre saker kan det være aktuelt å etterforske nettverk. Under etterforskningen mot kriminelle nettverk er det ofte nettopp trafikkdata - og analysen av dette – som gir en oversikt over det aktuelle kriminelle nettverk. Ikke minst er dette aktuelt i forbindelse med bekjempelse av organisert kriminalitet.

Hva angår type data, lagringstidens lengde og vilkårene for at politiet og påtalemyndigheten bør få tilgang til tilbyders data har vi i utgangspunktet ingen kommentar til, annet enn at lagringsperioden ikke bør være kortere enn den er i dag. (3- 5 mnd.) Politi- og påtalemyndigheten må således også i fremtiden kunne få ut trafikkdata minst så lenge som i dag så fremt øvrige vilkår er tilstede.

Politiets behov for datalagring utenfor etterforskning (Avsnitt 4)

Utenfor etterforskning innhenter politiet en betydelig mengde trafikkdata innen det tema som går under navnet Redningstjeneste.

Ved søk etter savnet person benytter politiets Redningstjeneste/HRS sine avtaler med Telenor og Netcom angående sporing av mobiltelefoner. Politiet sender i disse tilfellene anmodningen om sporing av mobiltelefonnummer til HRS. Dette er opplysninger som går under innhenting av etterretningsinformasjon og benyttes i de fleste tilfeller hvor en person er savnet. Redningstjenestens oppgaver er kun å redde mennesker i akutt nød. Trafikkdata innhentes i nåtid - eventuelt fra tidspunkt en person er meldt savnet. Hovedregelen er at disse trafikkdata er mindre enn en uke gamle - kanskje bare en dag gammel.

Dersom innhenting av trafikkdata skal være særlig aktuelt i denne forbindelse må dette skje så raskt som mulig, slik at liv kan berges.

Denne innhenting av trafikkdata går på sporing av i hvilket område mobiltelefonen befinner seg/siste kjente område og er ofte avgjørende i forhold til organisering av leteaksjonen.

En antar at muligheten for innhenting av trafikkdata til redningsformål vil bestå uavhengig av om datalagringsdirektives vedtas eller ikke, idet det her er snakk om kort lagringstid uansett. Men vi ønsker å understreke viktigheten av tilgang til slike data.

Det kan imidlertid ikke understrekes godt nok at det er desto mer viktig at redningstjenesten v/HRS eller LRS (politiet) får disse data raskes mulig. Vi sitter ikke med statistikk over hvor mange ganger rask tilgang til trafikkdata har berget liv, men en regner med at dette i mange redningsaksjoner har vært av avgjørende viktighet.

De konkrete spørsmål. (Avsnitt 6)

Spørsmål 1

....hva som evt skal lagres.

Ingen kommentarer annet enn de punktene (4.4.1 til og med 4.4.6) som er ramset opp i høringsnotatet. Høringsnotatets innhold tiltres.

Spørsmål 2

...lagringstid.

Inntil 1 års lagringstid vil i de fleste saker være tilfredsstillende når det gjelder samtaledata.

...ikke skille etter teknologi.

Ingen ytterligere kommentar. Høringsnotatets innhold tiltres.

JURIDISKE AVVEININGER

Generelt

Fra et etterforskningssynspunkt og for å gi politiet et best mulig etterforskningsverktøy er det åpenbart at lagring av trafikkdata har stor betydning. Desto mer informasjon man kan innhente og jo lengre denne finnes lagret, desto større betydning vil dette kunne ha for etterforskningen av en rekke saker. Politiets oppgave er blant annet å avdekke og oppklare straffbare forhold og da vil tilgang til lagrede trafikkdata kunne ha avgjørende betydning.

Spørsmål 3 (Avsnitt 6)

Det er foreslått at utlevering av trafikkdata bare bør kunne pålegges dersom det straffbare forholdet har en strafferamme på fengsel i 3 år eller mer. Den foreslåtte regel har sin bakgrunn i datalagringsdirektivets artikkel 4 om at trafikkdata bare skal utleveres i særlige saker, dvs. at trafikkdata bare skal være tilgjengelige for bekjempelse av grov kriminalitet. Regelen er en skjerpelse i forhold til dagens rettstilstand.

Begrensningen til forhold som har en strafferamme på mer enn 3 år er etter vårt syn ikke hensiktsmessig. En strafferamme gir selvfølgelig uttrykk for hvor alvorlig samfunnet ser på den kriminelle handlingen i alminnelighet, men konkret vil det lett kunne tenkes handlinger som i realiteten fremstår som alvorlige selv om strafferammen er under 3 år.

Det kan for eksempel tenkes at gjentatte straffbare handlinger hvor strafferammen er lav, men som samlet sett fremstår som mer alvorlig.

Teknisk sett lar det seg vel gjøre konkret å angi straffbare forhold (særlige saker) med strafferamme under 3 år hvor utlevering av data vil kunne skje. Den oppregningen som er gitt i høringsnotatet er etter vårt syn ikke tilstrekkelig. Den har blant annet ikke med handlinger som rammes av straffelovens § 227, 1. straffalternativ, § 219. ledd, § 222, 1. ledd, 1 straffalternativ, § 200 1. og 2. ledd, § 201, § 216 og § 342. Det må antas at det i tillegg til de her angitte bestemmelser er en rekke andre som også bør være med i en slik oppregning.

Et moment i mange saker er at de straffbare handlinger har sitt uspring i /utføres ved bruk av eller ved hjelp av elektronisk kommunikasjon. Det ville da være svært uheldig om man ikke kunne sikre bevis ved innhenting av de dataene som tilbyder har lagret uavhengig av strafferamme.

Etter vårt syn bør det ikke fastsettes noen strafferamme for å kunne innhente trafikkdata. Det bør heller ikke sondres mellom forbrytelser og forseelser. Begrensingen må ligge i en betraktning om at trafikkdata er nødvendig sett i forhold til den etterforskning som skal utføres og vurdert ut i fra en forholdsmessighetsvurdering.

Spørsmål 4 (Avsnitt 6)

Vi er av den oppfatning at dagens rettstilstand bør beholdes uendret. Det vises til Riksadvokatens brev av 02010 hvor det redegjøres for dagens rettstilstand. En ytterligere skjerpelse i forhold til dagens rettstilstand vil gjøre det vanskeligere med innhenting av de lagrede opplysninger. Dette kan ikke være ønskelig sett ut fra et etterforskningsmessig perspektiv.

Dersom det innføres en regel med krav om skjellig grunn til mistanke er det etter vårt skjønn viktig at dette vilkår ikke knyttes mot konkret person, men det må være tilstrekkelig at det er mistanke om at en straffbar handling er begått. Fra mange saker har man erfaring om at innhenting av trafikkdata nettopp er viktig for å avdekke en gjerningsmann. Noe annet ville innskrenke muligheten til effektiv etterforskning i saker med ukjent gjerningsmann.

Spørsmål 5

...en videreføring av det delte tilsynsansvaret mellom Post- og teletilsynet og Datatilsynet.

Ingen ytterligere kommentar. Høringsnotatets innhold tiltres.

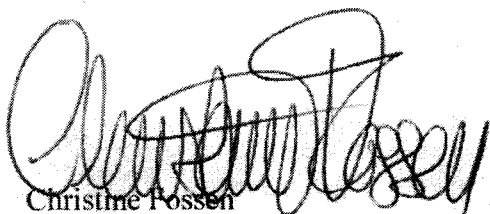
Spørsmål 6

...andre myndigheters tilgang til data...

Det vises til høringsnotatet side 47, 2. avsnitt.

Vi har ingen andre kommentarer enn dette.

SØNDRE BUSKERUD POLITIDISTRIKT



Christine Fossen

Jan Erik Strøm
visepolitimester



POLITIET

POLITIDIREKTORATET	
31 MAR 2010 ²	
Arkiv: 08-13	Arkivkode: 008
Saksnr. 16/134	Dok.nr. 18

MOTTATT
31 MAR 2010

Politidirektoratet
Postboks 8051 Dep.
0031 OSLO

Dens referanse
2010/00134-2 008

Vår referanse
2010/00212-2 008

Dato
25.03.2010

Høring om datalagring

EU's Datalagringsdirektiv ble vedtatt 15. mars 2006. Direktivet gir regler for lagring av trafikkdata fra telefon, mobiltelefon og epost, og innebærer lagring av identiteter, tidspunkt og lokaliseringsdata, innholdet i kommunikasjonen lagres ikke. Minstetid for lagring er 6 måneder, lengstetiden er 2 år.

Datatilsynet har pr. i dag pålagt teletilbyderne å slette trafikkdata etter noen uker, for kommersielle hensyn får de lagre data en kortere periode, dette for å kunne dokumentere trafikk i forbindelse med fakturering og eventuelle tvister med kunder. En teleoperatør kan i prinsippet slette alle data og etablere helt anonyme løsninger.

I EU trådte direktivet i kraft 15. september 2007, medlemslandene kunne utsette gjennomføringen til 15. mars 2009. Hittil er direktivet ikke innlemmet i EØS-avtalen. Regjeringen skal beslutte om direktivet skal innføres i norsk rett.

Formålet med direktivet er at de lagrede opplysningene skal kunne benyttes til å bekjempe kriminalitet og terrorisme. Kritikerne av direktivet mener det representerer en svekkelse av personvernet og et urimelig inngrep i privatlivet.

Fra dette politidistriktets vedkommende bemerkes at innføring av direktivet vil gi politiet en viktig mulighet til å forebygge og bekjempe kriminalitet og terrorisme. Datalagring som foreslått er ikke overvåking, det understrekes at innholdet i kommunikasjonen ikke lagres, og det er viktig å holde klart skillet mellom trafikkdata og innholdsdata. Videre vises til at hvis Norge ikke godtar Datalagringsdirektivet vil norsk politi få en dårligere mulighet til å bekjempe kriminalitet enn våre europeiske kolleger, som igjen vil kunne medføre økt kriminell aktivitet i Norge også utført av borgere fra andre land.

Innføring av Datalagringsdirektivet vil ikke innebære noe radikalt nytt i Norge. Innenfor de rammer dagens lagringstid setter her i landet vil politiet som ledd i etterforskning også i dag kunne innhente visse trafikkdata fra teletilbyderne, og denne muligheten har bl.a. vært benyttet til å oppspore savnede personer. Lokalisering av personer til gitte tidspunkt kan bidra til å bevise straffskyld så vel som til å frifinne. Som i dag vil det være en forutsetning at det foreligger mistanke om en straffbar handling, følgelig vil innsyn som foreslått kun

gjelde et mindre antall personer som er under etterforskning i forbindelse med en straffesak. Således vil Datalagringsdirektivet innebære lite nytt, den vesentlige forskjellen vil være lagringstiden av data. Det bemerkes for øvrig at politiet i en årrekke har hatt adgang til å benytte telefonavlytting som ledd i etterforskning, noe som innebærer tilgang til innholdsdata, og det påpekes at Datalagringsdirektivet ikke vil medføre noen endring i dette.

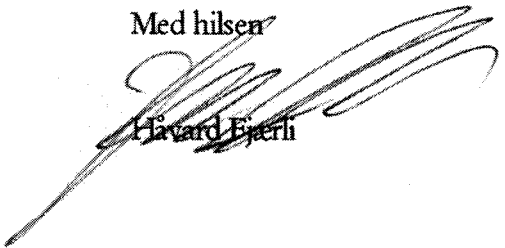
Oppsummering

Innføring av datalagringsdirektivet i Norge vil gi politiet en viktig mulighet til å forebygge og bekjempe kriminalitet og terrorisme. Dersom politiet skal få tilgang til data fra teleoperatør er det en forutsetning at det foreligger mistanke om en straffbar handling. Innsyn vil således bare gjelde for et svært lite antall personer som er under etterforskning i forbindelse med en straffesak. Når politiet pågriper en mistenkt, vil trafikkdata fra vedkommendes bruk av Internet, telefon, mobiltelefon, e-postadresse gi opplysninger om hvem mistenkte har kommunisert med. Politiet kan bruke opplysningene for å ta bakmenn og andre involverte i alvorlig kriminalitet – s.eks: menneskehandel, smugling av narkotika, sprit og tobakk, internet-relaterte overgrep mot barn, mobil vinningskriminalitet

Ved å si nei vil Norge bli en frihavn for kriminelle, fordi norsk politi får en dårligere mulighet til å avdekke kriminelle handlinger enn våre europeiske kolleger.

Datalagringsdirektivet lagrer ikke innholdet i kommunikasjonen og er ikke et steg nærmere overvåkningssamfunnet.

Med hilsen



Håvard Ejerli



POLITIET

MOTTATT

30 MAR 2010

Politidirektoratet
Postboks 8051 Dep
0031 OSLO
Norge

POLITIDIREKTORATET	
30 MAR 2010 3	
Arkiv 08-13	Arkivkode 008
Saksnr. 10/134	Dok.nr. 17

Deres referanse
2010/00134-2

Vår referanse
2010/00381-2 008

Dato
24.03.2010

Høring om datalagring

Det vises til Deres brev av 22.02.10 samt Samferdselsdepartementets høringsbrev av 8. januar 2010 om implementeringen datalagringsdirektivet.

Det bør ikke være ukjent for noen at det for politiets hovedformål om å forebygge og bekjempe kriminalitet, er av avgjørende betydning at datalagringsdirektivet implementeres i Norge.

Politimesteren vil kunne mene meget om avveiningen av personverninteresser mot hensynet til å sikre verktøy som muliggjør en effektiv bekjempelse av alvorlig kriminalitet. Man vil imidlertid her begrense seg til å fastslå at det i realiteten dreier seg om en mindre "reduksjon" i vernet av den personlige integritet.

I samfunnsdebatten får man blant enkelte av direktivets motstandere inntrykk at det er innholdet i kommunikasjonen som skal sikres laget, og ikke bare trafikken.

Politiet kjenner bedre enn noen den betydning tilgangen til trafikkdata har, og vil komme til å ha, for oppklaring og forebygging av alvorlig kriminalitet.

I denne avveiningen og vektingen av til dels motstridende interesser, må hensynet til samfunnsbeskyttelsen og behovet for effektivt å kunne bekjempe alvorlig kriminalitet være avgjørende.

Det synes også blant enkelte å være en feilaktig oppfatning at implementeringen av direktivet vil innebære vesentlige inngrep i personvernet utover dagens situasjon, herunder gi politiet adgang til informasjon man i stor grad ikke innehar i dag. Som fremhevet i høringen flere steder lagres slik informasjon allerede i dag og politiet har hjemler for tilgang til denne informasjonen.

Det nye ligger i at det er for myndighetenes interesse og bruk trafikken skal lagres, og ikke bare for fakturerings- eller kommunikasjonsformål som i dag.

I debatten om direktivet er det i den forbindelse at stor betydning at det foreligger klare trekk ved markedet at tilbyderne av trafikkdata i mindre utstrekning fremover vil ha behov for å lagre trafikken av faktureringshensyn. Man står altså overfor en situasjon hvor mangel på lovregulering i nær fremtid vil føre til at nytteverdien av straffeprosessloven § 215a blir liten ved at det ikke finnes data å "fryse".

Troms politidistrikt

Politimesteren, besøk: Grønnegt. 122
Post: Postboks 6132, 9291 TROMSØ
Tlf: 77 69 85 00 Faks: 77 61 04 04
E-post: post.troms@politiet.no

Det er etter vår mening et ikke uvesentlig moment at de trafikkdata som ønskes lagret, benyttes aktivt av kriminelle for å begå alvorlige forbrytelser på tvers av landegrensene. Herunder begås alvorlige seksuelle overgrep gjennom internettrafikk overfor et stort antall barn i ulike land, uten av overgriperne trenger å forlate egen bopel. Det dreier seg altså om alvorlig kriminalitet som ikke var mulig uten fremveksten av den teknologi EU gjennom direktivet ønskes lagret sporene av.

Datalagringsdirektivet er og vil i løpet av kort tid implementeres i EU-landene. At norsk politi i fremtiden gis dårligere betingelser enn våre nærmeste samarbeidspartnere, vil foruten å svekke vår evne til kriminalitetsbekjempelse også vanskeliggjøre det internasjonale politisamarbeidet.

Politiet erfarer også at trafikkdata er av avgjørende betydning i redningsaksjoner og for å etterspore savnede personer. Det finnes også en rekke eksempler på at trafikkdata kan sjekke personer "ut av saken" og i ytterste konsekvens hindre uriktige domfellelse.

Troms politidistrikt har ikke oversikt over omfanget av egen bruk av trafikkdata, herunder andelen saker dataen har betydning for innhentingsformålet. Det registreres at "Metodekontrollutvalget" har lagt til grunn at trafikken har betydning i ca. 40 % av de saker hvor det innhentes. Dette samsvarer godt med vår oppfattning av "treffprosenten".

Tradisjonelt har trafikkdata i størst utstrekning vært innhentet i narkotikasaker. I stadig større utstrekning ser vi nytteverdien av trafikkdata ved etterforskning av seksuelle overgrep og alvorlig vinningskriminalitet. Man har allerede erfaring med trafikkdata som uvurderlige hjelpemiddel i kampen mot de mobile vinningskriminelle.

Politimesteren deler departementet forslag til hvilke typer data som bør lagres, jf høringsbrevet punkt 4.4.

Når det gjelder lagringstiden lengde, må det avgjørende være at lagring ikke pålegges lengre tilbake i tid enn nødvendig i forhold til hensynet bak direktivet. Minstetiden på 6 måneder som angis i direktivet vil etter vår oppfatning være tiltrekkelig i langt på vei de fleste narkotika og vinningssaker som begrunner innsyn i trafikkdata. I grove sedelighetssaker og saker med organisert kriminalitet ser man imidlertid relativt ofte at trafikkdata er av betydning for å avdekke omfanget av de straffbare forhold.

Man registrerer at våre nordiske naboer har innført eller foreslår lagringsplikt i ett år. Lagringsplikten bør ikke under noen omstendigheter settes kortere enn dette i Norge, da det etter vår oppfatning som nevnt ovenfor ligger en betydelig fordel i likt regelverk landene imellom.

Det vil jo også ligge muligheter for senere utvidelse av lagringstiden dersom erfaringene i Norge og nabolandene dokumenterer slikt behov.

Videre synes det fornuftig ikke å skille på lagringstid etter type teknologi. Politimesteren deler departementet oppfatning av at den er en fordel med en teknologinøytral regulering.

Hva angår vilkår for utlevering av trafikkdata til politiet gir politimesteren sin tilslutning til forslaget om en strafferamme på 3 år. Som foreslått av departementet suppleres dette med oppregning av enkelte andre straffebud med lavere strafferamme hvor behovet for innhenting av trafikkdata erfaringsmessig har betydning for oppklaring og forebygging av

kriminalitet. Politimesteren har ikke synspunkter på lovovertrедelser utover de som der er oppregnet, jf høringsens punkt 4.12 og forslaget til endring av straffeprosessloven § 210.

Politimesteren er imidlertid sterkt uenig i departementets forslag hvor det kreves at noen konkret person med skjellig grunn kan mistenkes, jf høringsbrevet side 48/49.

Forslaget vil i tilfelle innebære en vesentlig begrensning i adgangen til å innhente trafikkdata i saker hvor dette erfaringsmessig har stor betydning.

Det må være tilstrekkelig som dagens regelverk rundt beslag og utleveringspålegg, at det foreligger skjellig grunn til mistanke om en straffbar handling og dataene "antas å ha betydning som bevis".

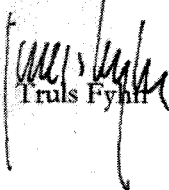
Til illustrasjon vil forslaget bety følgende i saker hvor ingen konkret person kan mistenkes:

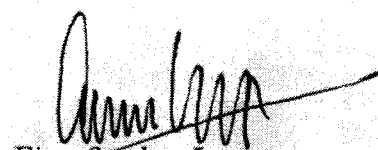
- Ved etterforskning av grove seksuelle overgrep over internet vil politiet ofte kunne sitte med en eller flere IP-adresser som sentralt bevis. Datatrafikken fra denne adressen vil i tilfelle ikke kunne innhentes.
- På åstedet for et drap/voldtekt finner politiet en mobiltelefon med ukjent/uregistrert eier. Utover det politiet finner på selve mobilen vil politiet ikke kunne hente informasjon fra basestasjoner (bevegelsene i forkant) eller trafikkdata.
- En bensinstasjon på et relativt øde sted ranes midt på natten. Innhenting av basestasjonstrafikk i område vil ikke være mulig.

Det er således vår sterkeste anbefaling at lovgiver begrenser til å kreve skjellig grunn som i dag og at begrensningen for politiet knytter seg til å overbevise domstolen om at tvangsmidlet vil være av vesentlig betydning for etterforskningen.

For de øvrige deler av forslaget har politimesteren ingen merknader.

Med hilsen


Truls Fyhn


Einar Sparboe Lysnes
politinspektør

Saksbehandler:
Einar Sparboe Lysnes
Tlf: 77698650 / 90965390



POLITIET

MOTTATT

30 MAR 2010

Politidirektoratet
Postboks 8051 Dep
0031 OSLO

POLITIDIREKTORATET	
30 MAR 2010 ³	
Arkiv 08-13	Arkivkode 008
Saksnr. 10/134	Dok.nr. 16

Deres referanse
2010/00134-2 008

Vår referanse
2010/00180-2 008

Dato
25.03.2010

HØRINGSUTTALELSE OM DATALAGRING

Det vises til Politidirektoratets brev av 22. februar 2010 hvor det bes om innspill på politiets behov for datalagring.

Follo politidistrikt vil først få takke for den forlengede høringsfristen til fredag 26. mars 2010, kl. 08:00, gitt ved e-post fra Bente Storruste av 23. mars 2010.

Politidistriktet har erfaring med at informasjon som kunne hatt bevismessig betydning ikke har vært tilgjengelig fordi den har vært slettet. Innføring av datalagring *utover* kommunikasjons- eller faktureringsformål ses på som et viktig og nødvendig verktøy for mer effektivt kriminalitetsbekjempelse, men kan også være en kilde for å utelukke straffeskyld (alibisjekk), eller for å avdekke falske tilståelser.

Kommentarer til pkt. 1 - 4 i Deres brev:

1. For å kunne avdekke saker om barnepornografi på Internett bør det vurderes en mulighet for å kunne innhente informasjon om gitte webadresser som har vært besøkt, men slik at innholdet ikke skal kunne sees. Innholdet vil evt. kunne avdekkes i etterfølgende undersøkelse av vedkommende datamaskin. Det er her snakk om svært samfunnsskadelig kriminalitet hvor hensynet til avdekking og oppklaring må veie tungt. Hvis en for denne type informasjon krever skjellig grunn til mistanke mot en bestemt person vil personvern hensyn kunne ivaretas. Folk flest vil også ha forståelse for en utvidet adgang for å kunne avdekke denne type saker.
2. Departementenes forslag til lagringstid (6 mnd.) ansees for kort - så kort at den ikke skiller seg vesentlig fra dagens ordning. EU - direktivet åpner for en adgang fra 6 mnd - 2 år. Departementene legger seg altså i nedre sjikt. Follo politidistrikt mener personvern hensynene kan ivaretas selv med en lengde på 2 år, men ser at det kan være hensiktsmessig å legge seg på samme nivå (1 år) som de medlemslandene som allerede har implementert direktivet. Under enhver omstendighet advares det mot kortere lagringstid enn det de andre landene har innført. Kortere lagringstid her til

Follo politidistrikt

Politimesteren

Post: Pob 3390, 1402 SKI, Norway

Tlf: 64 85 16 00 Faks: 64 85 17 26

E-post: post.follo@politiet.no

lands kan oppfattes som et mildere regime for kriminelle, slik at de velger å begå kriminalitet her fremfor i de andre EU – landene som har innført eller er i ferd med å innføre 1 års lagringstid. Kortere lagringstid her til lands enn i øvrige EU-land vil også kunne medføre færre rettsanmodninger fra utlandet om beslag i teledata fordi de aktuelle medlemslandene ser at tiden er gått ifra en, noe som indirekte kan bety tap av bevis mot for eksempel mobile vinningskriminelle. Like regler vil gjøre kampen mot grenseoverskridende organisert kriminalitet mer oversiktlig, noe som forhåpentligvis vil kunne stimulere til tettere politisamarbeid på tvers av landegrensene.

Fra Oppgård lensmannskontor ble det i 2004 etterforsket saker mot utenlandske mobile vinningskriminelle bander. Disse hadde spesialisert seg på å bryte opp spilleautomater. Utpå høsten samme år oppklarte lensmannskontoret et par slike saker og så samtidig en sammenheng med tilsvarende forhold på Nesodden fra april 2004. Når lensmannskontoret da hadde behov for basestasjonsopplysninger var trafikkdataen slettet.

I en drapssak som Frogn lensmannskontor har etterforsket siden sommeren 2008 kom det etter hvert frem informasjon om til da "ukjente" mobiltelefoner som hadde vært i bruk. Det viste seg imidlertid at det hadde gått mer enn tre måneder da politiet oppdaget dette, slik at viktig lokaliseringinformasjon og trafikkdata gikk tapt.

I en voldssak fra Ski sentrum fra 2008 ble det innhentet trafikkdata knyttet til mobiltelefonbruk innledningsvis. Tre mistenkte ble senere tiltalt. Etter hvert som etterforskningen pågikk så man at det hadde vært flere personer involvert i voldsepisoden, men tiden hadde da løpt ut for innhenting av trafikkdata for disse. Dersom lagringstiden hadde vært på 6 mnd. eller mer kunne materialet ha dannet grunnlag for videre etterforskning som igjen kunne ha medført at et større antall personer hadde blitt tiltalt.

I den såkalte "Lommemannssaken", som Follo politidistrikt har ansvaret for, antas det at i alle fall en henlagt sak kunne ha vært oppklart om ikke teledata hadde vært slettet.

3. Follo politidistrikt har ikke noe å bemerke til alternativene til den generelle strafferammen som foreslås, men er av den oppfatning at 3-års grensen er for høy, bl.a. vil legemsfor nærmelser med skadefølge falle utenfor. Dette kan slå uheldig ut i forhold til etterforskningen av voldssaker som for øvrig er særlig prioriterte. Det foreligger ikke slike kvalifikasjonskrav etter strpl. § 203. Det virker også inkonsekvent med et så strengt inngangsvilkår når en ellers i straffeprosessen for eksempel opererer med "fengsel i 6 måneder" (strpl. § 171), eller "frihetsstraff" (strpl. § 192).

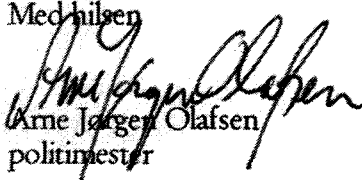
Follo politidistrikt kan ikke se gode grunner for at kompetansen skal legges til retten alene – uten hastekompetanse tillagt påtalemyndigheten som ofte ellers er løsningen.

4. Utformingen "skjellig grunn til mistanke" mot en bestemt person vil i praksis innebære innsnevring i forhold til dagens ordning, noe som klart må være i strid med formålet til direktivet. "Skjellig grunn til mistanke" som ikke retter seg mot en

bestemt person er bedre, men vil kunne hindre søk i redningsøyemed eller søk for å sjekke personer ut av saken.

For noen år tilbake ble det funnet et større narkotikaparti i en skog i Follo politidistrikt. Narkotikaen bar preg av å ha ligget der en god stund. Saken ble ikke oppklart, men kunne kanskje ha fått et annet utfall dersom politiet kunne gått bakover i tid og studert lokaliseringsinformasjon fra området.

Med hilsen


Arne Jørgen Olafsen
politimester

Saksbehandler:
Frode Marius Ruud
Tlf: 64851757

Kopi til:
FEE



POLITIET

Politidirektoratet
Pb 8051 Dep
0031 Oslo

MOTTATT
29 MAR 2010

POLITIDIREKTORATET	
29 MARS 2010	
Arldr: A08-13	Arldrkode: 608
Saksnr: 10/00134	Doc.nr: 14

Ders referanse
2010/00134-2 008

Vår referanse
Pfb Odd Arve solvåg

Dato
24.03.2010

Høring om datalagring

Det som er bedt om er særlig innspill på er politiets behov for datalagring. Vårt behov vil forsøkt synliggjort ved eksempel på saker hvor dette har vært aktuelt og vil bli aktuelt, å innhente denne typen informasjon.

Det som i dag blir lagret av trafikkdata når det gjelder telekommunikasjon fremstår som nødvendig for å kunne benytte seg av kommunikasjonskontroll på telefon og mobiltelefon. Uten den informasjonen kan det bli svært vanskelig å identifisere enheter som det er behov for å ha kontroll med. Slik som det er beskrevet i høringsnotat om hvilke data som skal lagres vil dette være tilstrekkelig, jfr. notatets pkt. 4.4.1 og 4.4.2.

Når det gjelder lagring av kommunikasjon som foregår med datamaskiner, for eksempel IP-adresser, er det i dag svært vanskelig å skaffe seg informasjon om brukere dersom forholdet overstiger tre uker. Slik som det er beskrevet i høringsnotat om hvilke data som skal lagres vil dette være tilstrekkelig, jfr. notatets pkt 4.4.3, 4.4.4 og 4.4.5.

I forhold til lagringstiden er vi av den oppfatning at det ikke bør skilles på teknologi. Dette begrunnes i at teknologiene går over i hverandre i mange sammenhenger. For eksempel det benyttes mobiltelefon som modem for å gi datamaskin tilgang til Internet. Videre vil eventuelt lovverk være bedre rustet til å fange opp teknologiutviklingen. Som ett minimum er vi av den oppfatning at det bør være minimum lagringstid på 1 år.

De lovbrudd som går inn i det generelle kravet vil i hovedsak være tilfredsstillende, men der finnes også andre lovbrudd som det er nevnt som bør inn i denne sammenhengen. Det er verdt å merke seg at andre land har differensiert lagringstiden, enten kortere eller lenger. Som hovedregel bør vi følge det som er utgangspunktet i notatet, men der bør, i lovverket ved eventuell implementering, gis en åpning til å innhente lagret informasjon i spesielle situasjoner.

Slike spesielle situasjoner kan være i finne frem til savnede personer, personer som er rømt fra fengsel eller som forsøker unndra seg fengselsstraff eller straffeforfølgning. I tillegg til

Sogn og Fjordane politidistrikt

det generelle kravet om strafferamme på 3 år, må enkelte lovbrudd som er oppregnet i notatet også være med.

Det som ikke er nevnt er fornærmedes krav til rettssikkerhet. Det har vært fokus på lovbrøtterne og deres vern. Vi har sett i saker hvor det forekommer ID tyveri at det er behov for å bistå fornærmede med informasjon som kan avhjelpe den situasjon de har kommet i samtidig som det er med å oppklare saken. Videre har politiet som oppgave å identifisere fornærmede, blant annet i overgrepssaker på Internet. Disse sakene vil bli umulige om ikke politiet får tilgang til informasjon som er nevnt skal lagres.

Det er åpenbart for oss at arbeidet med hindre organisert kriminalitet vil bli betydelig svekket, om ikke umulig, dersom vi ikke kan ha tilgang til informasjon som omhandles i direktivet. Den organiserte kriminalitet rammer samfunnet generelt og kan ramme enkelt personer spesielt. Vi har over de siste årene sett at bruken av kryptert e-post øker mellom de kriminelle. Dette er ett forhold som i utgangspunktet er vanskelig nok å håndtere, og vil bli umulig uten den informasjon som er foreslått lagret. Annen kommunikasjon som blir benyttet mellom kriminelle er meldingstjenester, og som vi ikke kan få tak i uten at vi klarer å identifisere anleggene og identitetene de benytter. Det kan vi klare ved informasjonen som er foreslått lagret.

I tillegg vil forhold som gjelder rikets sikkerhet og terror bli vanskelig å avdekke. Når vi vet at flere av grupperinger som utgjør en slik trussel, benytter seg av den type kommunikasjon hvis data er foreslått lagret. Så er vi i en situasjon at dataene ikke er tilgjengelig og vi vil ikke være i stand til å forhindre straffbare forhold mot samfunnet.

Et spørsmål som er betimelig å stille seg er hvordan vil vårt forhold til andre lands myndigheter i saker hvor vi ikke kan bidra med opplysninger. Vi er avhengige av opplysninger fra andre land i mange saker, for eksempel overgrep mot barn på Internet. Vil vi fortsatt få disse nødvendige opplysningene for å kunne oppklare disse sakene?

Det er bedt om en kommentar til om det skal være et lovfestet krav til vilkåret om skjellig grunn til mistanke. I dag er kravet at det kan tas beslag i noe som kan antas ha betydning som bevis. Vi er av den oppfatning at slik må det fortsatt være. Reglene som regulerer forholdet i dag er i hovedsak gode nok. Vi må også huske på at det kan være behov for å sjekke personer ut av en sak. Det vil si at vi også skal kunne bevise at personer er uskyldig. Vi må hindre at personer blir uskyldig dømt.

Med hilsen



Odd Arve solvåg
Politiførstebetjent

Saksbehandler:
Pfb Odd Arve Solvåg
Tlf: +47 57758836/91589988



POLITIET

Politidirektoratet
Postboks 8051 Dep
0031 OSLO

MOTTATT
29 MAR 2010

POLITIDIREKTORATET	
29 MARS 2010	
Arkiv:	Arkivkode:
8-13	008
Saksnr.	Dok.nr.
10/134	12

Deres referanse
2010/00134-2 008

Vår referanse
2010/00226-3 008

Dato
25.03.2010

Høring om datalagring

Det vises til deres brev av 22. februar 2010 m/vedlegg.

Generelt

Innledningsvis vil jeg bemerke at det er politikerne som tilslutt må trekke grensen for hva som skal være tillatt å lagre av historiske trafikkdata, både når det gjelder hva som kan lagres, hvor lenge og under hvilke vilkår politiet skal kunne nyttiggjøres seg dette.

Jeg er selvsagt klar over at politiets behov ikke nødvendigvis blir avgjørende ved en slik avveining, men det må være viktig for de som skal ta beslutningen hvordan politiet vurderer dette ut ifra sitt ståsted.

Politiets behov for trafikkdata og omfang.

Det er ingen tvil om at politiet de senere årene har sett et økende behov for å innhente trafikkdata i et større antall saker. Politiet i Asker og Bærum kan ikke tallfeste dette eksakt, men tallet er ikke ubetydelig. Det kan imidlertid bemerkes at innhenting av trafikkdata er et kostnadsspørsmål og at vi derfor vurderer nøye hvilke saker vi mener det er behov for å innhente data i.

Asker og Bærum politidistrikt deltar i samarbeidsprosjekt Grenseløs og arbeider målrettet mot mobile vinningskriminelle, særlig når det gjelder grove tyverier fra bolig. I denne typen saker har historiske trafikkdata i flere tilfeller vært avgjørende for oppklaring og senere domfellelse i sakene. I mange tilfeller opererer flere sammen i nettverk og det er viktig å få tatt flest mulig av de personene som begår så samfunnsskadelig kriminalitet som boliginnbrudd er. Vi har erfaring med at de involverte ikke innrømmer mer enn det de blir tatt for. Det er derfor helt avgjørende for håndteringen av denne typen saker at vi kan bruke trafikkdata som et verktøy for å knytte personer sammen og knytte personer til åstedene. Vi ser i mange saker at de faktiske opplysningene trafikkdata gir, i konfronterende sammenheng kan bidra til at siktede erkjenner både forhold og kjennskap til involverte personer. I flere saker vil trafikkdata også være viktig for domfellelse etter strl § 60 a – organisert kriminalitet og da særlig kravet om organisert kriminell gruppe.

Også i narkotikasaker ser vi at historiske trafikkdata kan ha avgjørende betydning. Hvilke

Asker og Bærum politidistrikt

Retts og påtale avdelingen, besøk: Kjørboveien 33
Post: Postboks 415, 1302 Sandvika
Tlf: 67 57 60 00 Faks: 67 54 86 34
E-post: post.askerogbaerum@politiet.no

Org. nr.: 947 131 613

basestasjoner telefoner har slått inn på, hvilke telefonnr som har hatt kontakt til hvilke tidspunkt sett i sammenheng med beslag, kan være avgjørende for å knytte personer til det straffbare forhold.

Helt konkret kan det nevnes at innhenting av trafikkdata på en nødsamtale i en kidnappingsak, gjorde at vi kunne "splitte" opp nødsamtalen, slik at vi fikk samtlige basestasjoner på kjøreturen. Dette gjorde at vi fikk avgjørende opplysninger for den videre etterforskning i saken.

Videre har politiet innhentet trafikkdata på flere telefoner som tilhørte siktede. Systematisering av denne ga oss siktedes ringemønster de siste månedene. Dette har også gitt oss viktige og avgjørende opplysninger for etterforskningen i saken.

Hva som eventuelt skal lagres:

Asker og Bærum politidistrikt slutter seg til departementets forslag i kapittel 4.4.1 - 4.4.5 og har ingen ytterligere kommentarer til det.

Lagringstid og forslag om å skille lagringstid etter teknologi:

Forslaget om å ikke skille lagringstid etter teknologi synes fornuftig.

Når det gjelder lagringstid vil man i mange saker ha behov for trafikkdata som er eldre enn 6 måneder. Hva angår mobile vinningskriminelle som opererer over tid vil det være mye å hente på å ha lenger lagringstid.

I grove narkotikasaker ser vi i flere tilfeller at det underveis i etterforskningen kan knyttes personer til beslaget, men hvor det er gått såpass lang tid at trafikkdata etter dagens regelverk og praksis er slettet.

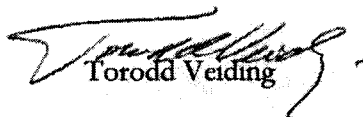
Oppregning av lovbrudd som er foreslått so alternativer til det generelle kravet om at handlingen skal kunne medføre fengsel i 3 år eller mer:

Politiet i Asker og Bærum slutter seg til de forslagene til lovbrudd som er foreslått av departementet. I tillegg bør det etter vår oppfatning vurderes om strl § 127 bør gi grunnlag for innhenting av trafikkdata. Likeledes om overtredelse av strl § 162 b (doping) bør med.

Utformingen av vilkåret om skjellig grunn til mistanke:

Etter vår oppfatning vil det være uheldig å begrense mulighet for innhenting av trafikkdata til tilfeller det er det er skjellig grunn til mistanke knyttet til en bestemt person. Når det etter dagens praksis kan vises til flere eksempler på at trafikkdata kan være avgjørende som bevis, vil det være svært uheldig med en begrensning som foreslått.

For øvrig kan en tenke seg at det i alvorlige saker kan være behov for innhenting av trafikkdata fra fornærmedes telefon/internettaksess. Det kan for eksempel dreie seg om alvorlig vold/drap uten kjent gjerningsmann hvor opplysninger fra fornærmedes telefon/pc vil gi viktig informasjon som kan lede fram til en eventuell gjerningsmann. I slike tilfeller vil det være uheldig om det var et vilkår om at det måtte foreligge skjellig grunn til mistanke mot en bestemt person.


Torodd Veiding

Saksbehandler:

Stine Karlsen

Tlf.: 67576953



POLITIET

Politidirektoratet
Postboks 8051 Dep.
0031 Oslo

MOTTATT

29 MAR 2010

POLITIDIREKTORATET	
29 MARS 2010	
Arnr: A08-13	Arkivnr: 008
Saksnr: 10/00134	Dokument: 11

Deres referanse
2010/00134-2

Vår referanse
2010/00739-2 008

Dato
24.03.2010

Høring om datalagring

1.0 Innledning

Hordaland politidistrikt er positivt innstilt til at datalagringsdirektivet innlemmes i EØS-avtalen. Etter Hordaland politidistrikt sitt syn vil en implementering av EUs datalagringsdirektiv i norsk rett være helt nødvendig for at politiet skal ha de nødvendige verktøy i bekjempelsen av alvorlig og organisert kriminalitet.

Datalagringstidens lengde har betydning både for politiets muligheter til å bekjempe alvorlig kriminalitet, personvernets totale belastning og for å sikre likt regelverk for det indre markedet i EU. Norge bør etter Hordaland politidistrikts oppfatning bestrebe seg på en mest mulig harmonisert datalagringstid med andre nasjoner innen EU.

2.0 Hva bør lagres og hvorfor?

Hordaland politidistrikt ønsker at abonnementsopplysninger lagres fordi:

- Politiets arbeid ofte er i etterkant av kriminelle handlinger
- Man unngår enkel anonymisering av elektronisk kommunikasjon

Slik vi ser det så innbefatter Samferdselsdepartementets høringsutkast punktene 4.4.1- 4.4.5 de punkter som er aktuelle for politiet å hente ut data fra. Vi kan ikke se at det er behov for ytterligere datainnsamlingsgrunnlag.

Hordaland Politidistrikt ønsker at historiske data lagres over tid fordi:

- Mange saker blir anmeldt sent (for eksempel sedelighetssaker) eller at ny informasjon kommer inn i sak over tid (mobile vinningskriminelle).

Hordaland politidistrikt

- b. Elektronisk kommunikasjon er i stadig utvikling og det gir rom for nye "områder" for kriminelle handlinger (som for eksempel forum på internett, facebook m.m.). Det er ikke mulig for politiet å ligge i forkant for all utvikling. Politiet trenger derfor tid til å justere sine etterforskningsmetoder.
- c. Det gir mulighet for å finne forbindelser mellom eldre saker, eksempelvis saker av samme karakter som "lommemann" saken og profesjonell vinningskriminalitet.
- d. Man hindrer at politiet kommer i en posisjon hvor man "overlagrer" data pga frykt for at data går tap. Et eksempel på dette er det såkalte "Hylkjedrapet" utenfor Bergen i 2008 hvor all basetrafikk ble fryst pga politiet ikke visste hva de lette etter på det tidspunktet. Politiet måtte sikre all data da det kunne være e-spor man fikk bruk for i fremtiden. Det viste seg også å medføre riktighet, men politiet ble sittende igjen med mye overskuddsinformasjon.

3.0 Forslaget om å ikke skille lagringstid etter teknologi

Hordaland politidistrikt ser ikke et relevant grunnlag for å differensiere lagringstiden i forhold til teknologien som er benyttet i kommunikasjonen. Dette fordi at uavhengig av hvilken teknologi man taler om innenfor det tema datalagringsdirektivet omhandler, så er det snakk om flyktige data. Spor finnes gjerne på et medium, eksempelvis en hard disk, og dette føres videre til et annet medium som f.eks mobiltelefon. En kan dermed ikke skille lagringstiden. Det er også grunn til å være oppmerksom på at teknologien er i stadig endring, en spesifisering av teknologi i forhold til tidsbegrensning vil være med å problematisere fremtidige forsøk på innhenting av trafikkdata.

4.0 Datalagringstiden

Datalagringstiden er viktig for politiets kriminalitetsbekjempelse og personvernet både knyttet til den som er utsatt for lovbruddet, den som begår lovbruddet og allmennheten. Jo kortere datalagringstiden er, jo mer data tvinges politiet å kreve utlevert. I startfasen av etterforskningen av alvorlige lovbrudd vet som regel ikke politiet hvilken retning etterforskningen vil ta. Derfor samler politiet opplysninger bredt og prioriterer etterforskningsskrittene som sikrer opplysninger som vanskelig lar seg gjenskape på et senere tidspunkt. Hvis datalagringstiden er kort, krever det at politiet må sikre unødvendig mye data i denne fasen. Jo lenger datalagringstiden er, jo mer konkret kan politiet være i utleveringsbegjæringene og jo mer ressurseffektiv blir etterforskningen.

I enkelte alvorlige saker får ikke politiet kjennskap til saken før det er gått en tid. Ulike prosedyrer regulerer slike sakers fremvekst og videre behandling. Mange kommuner har opprettet voldtektsmottak hvor offeret kan få sikret biologiske og andre spor fra voldtekten. Dette er spor som lagres ved voldtektsmottaket mens offeret vurderer om saken skal politianmeldes. Det kan gå lang tid fra sporene ble sikret til politiet blir varslet. Når vedkommende anmelder saken, kan politiet hente sporene på mottaket. Hvis datalagringstiden er kort, vil de ulike trafikkdata som kan ha bevismessig betydning for saken være tapt.

Menneskehandelsaker stiller i samme kategori. I disse sakene gis offeret ofte en refleksjonsperiode før en eventuell anmeldelse til politiet. Kort datalagringstid kan føre til at refleksjonsperioden oversitter datalagringstiden, og politiet står uten viktige spor for å etterforske bakmennene for menneskehandelsaken og kontrollere fornærmedes og de anmeldtes forklaringer.

Internasjonalt er det stor fokus på internettbasert spredning av barneporno. Norge har ved flere anledninger deltatt i koordinerte internasjonale aksjoner for å straffeforfølge overgripere og identifisere barn som er utsatt for dokumenterte seksuelle overgrep. Informasjon innhentet fra slike aksjoner kan føre til nye aksjoner for å straffeforfølge andre overgripere og identifisere nye barn, eller skape bedre grunnlag for å identifisere barn.

Hvis Norge har kortere datalagringsbestemmelser enn samarbeidende nasjoner, står Norge i fare for å utelukke seg selv fra slikt samarbeid. Norge står også i fare for å bli en hemsko for andre nasjoners bestrebelser på å avdekke overgripere og identifisere barn som utsettes for seksuelle overgrep.

5.0 Strafferammens betydning for politiets tilgang til data

Departementet foreslår at utlevering av data bør kunne pålegges dersom det straffbare forholdet har en strafferamme på fengsel i 3 år eller mer. Dette er i samsvar med den definisjonen av alvorlig kriminalitet som er nedfelt i den europeiske arrestordre av 13.6.2002.

Vinningskriminalitet dominerer som kjent tallmessig i Norge. Politiet har gjentatte ganger blitt kritisert av politiske myndigheter fordi oppklaringsprosenten på hverdagskriminalitet som vinningskriminalitet er lav.

I European United organized crime report 2004 (EU-OCR 2004) fremheves det at organiserte kriminelle grupper i økende grad retter seg inn mot mengdekriminalitet som lommetyverier, butikkttyverier og bedragerier overfor enkeltpersoner. Dette er en utvikling basert på de kriminelle nettverkens økede fokus på lav risiko – høy profit.

De senere årene har også Norge opplevd en økning av utenlandske nettverk som er svært aktive innen forskjellige former for vinningskriminalitet. Fellesnevner har vært spesialisering innen en snever nisje, hyppig utførte forhold kombinert med stor mobilitet.

Ved simple tyverier, bilbrukstyverier og bedragerier ovenfor privatpersoner, banker og forretninger er strafferammen i dag 3 år. Dersom denne strafferammen opprettholdes i ny straffelov så er Hordaland politidistrikt enig med departementet i at en strafferamme på fengsel i 3 år eller mer kan legges til grunn. Dersom imidlertid strafferammen i ny straffelov senkes til 2 år for overnevnte lovbrudd, så bør dette også få betydning for den strafferamme som legges til grunn for pålegg om utlevering av data.

I etterforskning av tyverier vil det ofte i den innledende delen av etterforskningen være naturlig å subsumere forholdene som simple tyverier. En strafferamme på 3 år vil medføre at politiet ikke får data som kan være avgjørende for vurderingen av tyverienes grovhet.

Data av denne type vil kunne vise at det er de samme gjerningsmenn som opererer, men vil også kunne belyse om det er andre gjerningsmenn/bakmenn eller profesjonelle kriminelle nettverk som er involvert. Avhengig av situasjonen vil derfor dataene kunne bidra til domfellelse eller frifinnelse.

Hordaland politidistrikt anbefaler derfor at utlevering av data bør kunne pålegges dersom det straffbare forholdet har en strafferamme på fengsel i 3 år eller mer under forutsetning av at denne strafferammen opprettholdes for de overnevnte vinningskriminelle lovbrudd også i den nye straffeloven.

6.0 Eksempler hvor trafikkdata har vært sentralt for oppklaring av alvorlige straffesaker:

6.1 Bergen tingretts dom av 14.1.2010 – Omfattende seksuelt misbruk av barn

43 år gammel mann dømt til 10 års forvaring med en minstetid på 6 år for omfattende seksuelt misbruk av barn under 14 år og barn under 16 år, menneskehandel og produksjon av barnepornografi. Trafikkdata ble innhentet for tiltaltes mobiltelefon, for perioden fra løslatelse fra første fengslingsperiode, og frem til ny pågripelse. Dette ga bevis for fortsatt kriminell virksomhet - misbruk av gutter seksuelt, som igjen ledet til ny pågripelse og fengsling frem til hovedforhandling grunnet kvalifisert gjentakelsesfare.

6.2 Gulating lagmannsretts dom av 10.6.2009 – To innsatte organiserer innførsel av 2 større amfetaminpartier fra Litauen mens de soner lengre narkotikadommer i Bergen fengsel.

5 personer ble dømt til lengre fengselsstraffer for innførsel av 2 større partier med metamfetamin fra Litauen til Norge. To av gjerningspersonene sonet fengselsstraffer på gjerningstidspunktene. Retten la til grunn at det var de to innsatte i Bergen fengsel som hadde hatt de mest sentrale rollene i innførselen. Trafikkdata var et helt sentralt bevis i saken for å bevise knytningene mellom de siktede og kontakten med leverandøren i Litauen. Det ville trolig ikke vært tilstrekkelig bevis mot de 2 hovedmennene uten trafikkdata. Leverandøren i Litauen ville ikke blitt avslørt uten de opplysninger som fremkom av innhentet trafikkdata.

6.3 Bergen tingretts dom av 15.mai 2009 – 28 år gammel mann solgte større mengder amfetamin og narkotiske tabletter samtidig som han sonet en lengre dom i Bergen fengsel.

I perioden fra ca januar – desember 2008 kjøpte en 28 år gammel mann ca 316 gram amfetamin, ½ kilo hasj og over 3000 tabletter. Av dette videresolgte han ca ½ -parten til rusmisbrukere i Bergen. De straffbare forholdene skjedde samtidig som han sonet en lengre dom i Bergen fengsel og i forbindelse med at han hadde

permisjon fra fengselet. Trafikkdata var et sentralt bevis for å avdekke hvem tiltalte hadde hatt kontakt med når han var på permisjon og narkotikasalgene hadde funnet sted.

6.4 Gulating lagmannsretts dom av 14.12.2009 – Grov Menneskehandel med mindreårig albansk jente

3 personer domfelt for grov menneskehandel. 17 år gammel albansk jente utnyttet til prostitusjon. Trafikkdata var et helt sentralt bevis i saken for å avdekke knytninger mellom de siktede, reiseruter og knytning til fornærmede. Det antas med sikkerhet at ingen av de tiltalte ville blitt domfelt uten det bevismaterialet som ble avdekket gjennom innhenting av trafikkdata.

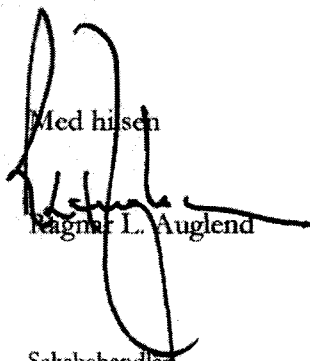
6.5 Gulating lagmannsretts dom av 11.4.2007 – Omfattende og profesjonell vinningskriminalitet – Prosjekt Albatross (ROK – Sak).

5 personer domfelt for til sammen ca 75 straffbare forhold, fortrinnsvis grove tyverier begått ved tyveriraid fra Lindesnes til Harstad. Trafikkdata var helt avgjørende bevis i saken. Uten trafikkdata ville det ikke vært mulig å knytte de siktede til åstedene. Det ville heller ikke vært mulig å knytte de siktede til hverandre i det omfang som ble avdekket gjennom innhenting av trafikkdata fra beslaglagte mobiltelefoner. Politiet ville ikke hatt bevis for at gjerningsmennene samarbeidet om tyveriene. Det antas med stor grad av sikkerhet at tilnærmet samtlige forhold ville blitt henlagt uten opplysningene som fremgikk av trafikkdata.

6.6. Norhordland tingretts dom av 22.6.2006 – Profesjonell vinningskriminalitet

Mann dømt til fengsel i 2 år for grovt tyveri fra butikk og grovt skadeverk. Gjentatte ganger domfelt og utvist fra Norge tidligere for tilsvarende lovbrudd. Trafikkdata var helt avgjørende bevis i saken. Uten trafikkdata ville det ikke vært mulig å knytte tiltalte til åstedene.

Med hilsen



Ragnar L. Auglend

Saksbehandler
Rudolf Christoffersen



POLITIET

Politidirektoratet
postboks 8051Dep
0031 OSLO

MOTTATT

26 MAR 2010

POLITIDIREKTORATET	
26 MARS 2010	
Saksnr. A08-13	Arkivnr. 008
Saksnr. 10/20134	Arkivnr. 10

Deres referanse
201000134-2 008

Vår referanse
2010/00285-2 513

Dato
23.03.2010

Unntatt offentlighet:
Offl. 14

Høring om datalagring

Det vises til Politidirektoratets brev av 22. februar 2010 hvor det blir bedt om innspill på Samferdselsdepartementets høringsbrev av 8. januar 2010 om datalagring.

Innledningsvis vil vi bemerke at høringsnotatet på en meget god måte angir de problemstillinger som datalagringsdirektivet reiser. Notatet inneholder også grundige drøftelser av de avveininger som må foretas før direktivet eventuelt blir implementert i norsk rett.

Vi lever i en globalisert verden og den teknologiske utviklingen går stadig raskere. Det innebærer også at kriminalitetsbildet er i forandring. Det stilles stadig nye krav til politiet. For å kunne imøtegå den nye kriminaliteten trenger politiet å oppdatere seg på ny teknologi og få muligheten til å benytte den teknologien som er tilgjengelig. Politiets tilgang til lagrede data vil i noen tilfeller være avgjørende for at man skal lykkes med sin oppgaveløsning.

Nord-Trøndelag politidistrikt innhenter allerede i dag lagrede data, og da i hovedsak i form av trafikkdata fra mobiltelefoner. Man ber da om trafikkdata for så lang tilbake i tid som disse er lagret, og det vil i praksis si i tre måneder for Telenor og fem måneder for NetComs kunder. Den informasjon som slike utskrifter gir har visst seg å være av stor verdi, og da særlig i oppklaringen av narkotikaforbrytelser, men også i vinningsforbrytelser. For vårt distrikt vil bruken av lagrede data være forholdsvis beskjeden ut fra det kriminalitetsbildet som vi har i dag.

Bruk av trafikkdata utenfor etterforskning kan være aktuelt i blant annet forsvinningssaker. Ofte er det da ikke behov for å gå like langt tilbake i tid som bruken av data under etterforskning.

Nord-Trøndelag politidistrikt

Retts- og påtaleenheten, besøk: Strandveien 38
Post: Postboks 2620, 7734 STEINKJER
Tlf: 74 12 10 00 Faks: 74 12 10 25
E-post: post.nord-trondelag@politiet.no

Org. nr.: 983 998 704
Bankgiro: 7694.05.11492

I forhold til de enkelte problemstillinger som er opplistet i Politidirektoratets brev har vi følgende kommentarer:

1. Presisering av hva som skal lagres:

Når det gjelder spørsmålet om hva som skal lagres vises det til høringsnotatets punkt 4.4.1 til 4.4.5. Nord-Trøndelag politidistrikt støtter departementenes forslag til hva som skal lagres og har ikke kommentarer utover dette.

2. Lagringstid og forslaget om å skille lagringstid etter teknologi:

Nord-Trøndelag politidistrikt støtter forslaget om at lagringstiden settes til ett år som er lagringstiden i våre naboland Finland og Danmark. Det er slik vi ser det også gode argumenter for å velge en lagringstid som er den samme uavhengig av valg av teknologi. I høringsnotatet er det vist til konkurransehensynet som ett argument for en slik løsning. Vi ser det også som en fordel i politiets kriminalitetsbekjempelse om lagringstiden er den samme for all teknologi som blir benyttet.

3. Oppregningen av lovbrudd som er foreslått som alternativer til det generelle kravet om at handlingen skal kunne medføre fengsel i 3 år eller mer.

Enkelte lovovertridelser er vanskelige å etterforske uten at man har tilgang til lagrete data. Det er slik vi ser det derfor av stor betydning at enkelte lovbrudd som har en lavere strafferamme på fengsel i 3 år eller mer også blir omfattet av data som kan pålegges utlevert. For vårt vedkommende ser vi at dette særlig kan ha betydning for narkotikaovertridelser og etterforskningen av seksuallovbrudd mot barn. Overtridelser av straffeloven § 390a er også en praktisk viktig bestemmelse som derfor også bør omfattes. Et eksempel på ny teknologi som vi har hatt erfaring med i det siste er nedlasting av programvare på mobiltelefoner som gjør at samtaler på telefonen kan avlyttes, og at man får tilgang til all kommunikasjon av tekstmeldinger på telefonen. Det vil være en grov integritetskrenkelse for den som opplever at mobiltelefonen blir avlyttet.

4. Utformingen av vilkåret om skjellig grunn til mistanke:

I høringsnotatet er flere alternative forslaget drøftet. Vi ønsker at man velger alternativet om at man lovfester vilkåret om skjellig grunn til mistanke, men ikke at dette må knytte seg til en konkret person. Hvis man velger alternativet om at "noen med skjellig grunn mistenkes" vil man få ut data i færre saker og det blir vanskeligere å oppklare saker der det ikke lar seg bevise at det foreligger skjellig grunn til mistanke som knytter seg til en bestemt person. Blant annet i etterforskningen av tyverier begått av mobile vinningskriminelle har man i innledningen av etterforskningen ofte fått opplysninger om en bestemt gjerningsperson. Hvis man må konkretisere at en bestemt person er mistenkt vil etterforskningen bli vanskeliggjort.

5. Forslaget om å videreføre det delte tilsynsansvaret mellom Post- og teletilsynet og Datatilsynet:

Under dette punktet støtter politidistriktet forslaget om at delingen mellom Post- og teletilsynet og Datatilsynet videreføres. Det er viktig at etatene avklarer områdene for sin tilsynskompetanse slik at man har klart definerte ansvarsområder.

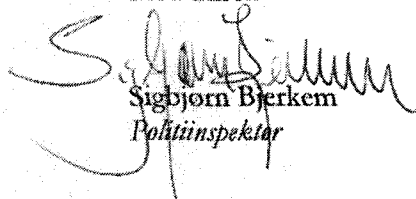
6. Andre myndigheters tilgang til data:

Dette spørsmålet reiser etter vårt syn en prinsipiell viktig problemstilling. Formålet med direktivet er å bekjempe kriminalitet og dette er en oppgave for politi og påtalemyndighet. Det er slik vi ser det et viktig prinsipp som ikke må uthules ved at man gir andre tilsynsorganer tilgang til data på samme måte som for politi og påtalemyndighet.

7. Innhenting av data for å avdekke pressens kilder:

Under dette punktet vises det til høringsnotatets drøftelse og politidistriktet har ikke særskilte kommentarer til dette punktet.

Med hilsen



Sigbjørn Bjerkem
Politinspektør

Saksbehandler:
Politiadvokat Jørgen
Aunet
Tlf: 74 21 20 45



POLITIET

Politidirektoratet
Postboks 8051 Dep.
0031 OSLO
Norge

MOTTATT

26 MAR 2010

POLITIDIREKTORATET	
26 MARS 2010	
Arkiv 108-13	Arkivkode 008
Saksnr 10/00134	Dok.nr 9

Deres referanse
2010/00134-2 008

Vår referanse
2010/00249-2 513

Dato
23.03.2010

Høring om datalagring

Det vises til politidirektoratets skriv av 22.februar 2010.

Etter vår oppfatning har politiet et stort behov for innføring av EUS datalagringsdirektiv i vårt arbeid med kriminalitetsbekjempelsen.

Det verste som kan skje er at datalagringsdirektivet ikke implementeres og teletilbyderne slutter å lagre data fordi deres eget behov for lagring ikke lenger er tilstede. Da vil vi ha dårligere tilgang til bevis enn i dag og da står vi utrolig dårlig rustet i kriminalitetsbekjempelsen

Når det gjelder behovet for tilgang til data for eksempel i redningstjenesten – blir det ofte innhentet (av HRS eller LRS) data på et nødrettslig grunnlag for å lokalisere personer i nød, men vi har ingen erfaringer med at man her trenger data langt bak i tid. Skulle det bli enda mindre lagring enn i dag vil det også for disse hendelsene få betydelige konsekvenser.

Det viktigste er at politiet nå klarer å beskrive de behovene vi har og vi tenker at Kripas undersøkelse om bruk av trafikkdata vil bli et vesentlig moment i politiets høringssvar.

Salten politidistrikt har i mange saker benyttet data som viktige bevis. En rekke kriminalitetsområder kan omhandles, men for oss er det mest nærliggende i forbindelse med denne høringen å trekke frem hvor viktig tilgangen til data er i bekjempelse av overgrep mot barn. På s. 19 vises det til at politiet har opplyst at det den senere tid har vært vanskeligere å etterforske internettrelaterte saker vedrørende overgrep mot barn pga den korte lagringstiden av data. Det problematiseres ikke noe videre rundt hvor alvorlig dette egentlig er.

Det problematiseres heller ikke noe om at det vil være svært uheldig dersom norsk politi gis dårligere metoder enn de fleste andre europeiske land- i en tid der vi holder på å ta inn over oss hvor grenseoverskridende kriminaliteten er.

Salten politidistrikt

I høringsnotatet pkt 4.1 beskrives en del viktig mht at teknologiutviklingen har gitt kriminelle nye muligheter til å kommunisere med hverandre ved planleggelse og utøvelse av kriminelle handlinger.

Et aspekt mangler. Når det gjelder seksuelle overgrep mot barn, spredning av overgrepbilder har teknologiutviklingen og særlig internett medført en "normalisering" av overgrep mot barn. En overgriper trenger ikke føle seg alene eller unormal. Man vil alltid finne likesinnede, som oppmuntrer hverandre.

Internett "tilrettelegger" i større grad for disse typene overgrep – og da er det ille at overgriperne i stor grad skal kunne verne sin identitet. Skal de kriminelle ha alle "fordelene" ved den teknologiske utviklingen – hva med ofrene?

Salten politidistrikt har pt under etterforskning en stor og alvorlig sak om overgrep mot barn. Overgrepene siktelsen gjelder har en strafferamme på 21 års fengsel. Saken skal behandles i retten i juni 2010.

Vi har uttalt til media at dersom det hadde foregått datalagring i henhold til Eus datalagringsdirektiv ville saken hadde et mye større omfang i og med at politiet da høyst sannsynlig ville kommet i kontakt med flere ofre.

Vi velger å ta inn vår beskrivelse av problematikken knyttet til datalagring relatert til denne saken

"På pc-en til 35-åringen som nå er siktet fant vi to identer/e-postadresser som siktede hadde brukt i internettkontakten med mange personer som vi mistenkte måtte være mindreårige gutter. Disse identene/e-postadressene var hovedsaklig brukt for å skaffe "venner", få kontakt og chatte med andre på Windows Live Messenger(MSN). Siktede hadde altså to forskjellige kallenavn/identiteter som han opererte med på Windows Live Messenger. Dette programmet gir brukerne mulighet til blant annet å sende og motta bilder og film, ha live-samtaler via webkamera, i tillegg til vanlig skriftlig samtale(chat).

Gjennom en av disse identene/e-postadressene gav han inntrykk av å være den han er, nemlig en 35 år gammel mann. Gjennom den andre identer/e-postadressen fremstilte han seg selv som en jente i 15-16-årsalderen.

Etter å ha hentet ut den informasjonen vi trengte fra pc-en til siktede, henvendte Salten politidistrikt seg umiddelbart til Microsoft for å få ut kontakt-/vennelistene til disse to identene/e-postadressene. Ved å kontakte Microsoft var vi sikre på å få ut komplette og korrekte lister.

Vi fikk raskt svar fra Microsoft, og det viste seg at de to identene til sammen hadde rundt 1250 kontakter/venner. Bare 188 av disse kontaktene tilhørte identer/e-postadressen der siktede opptrådte som seg selv. Resten tilhørte "jenta".

Vi sammenlignet vennelistene til de to og fant ut at 46 av kontaktene hadde lagt til både den "15-16-årige jenta" og 35-åringen selv som venner. På grunnlag av dette forsto vi at siktede hadde hatt kontakt med disse både som mann og jente, og derfor målrettet vi innsatsen mot disse kontaktene. Ut fra informasjon funnet på siktetes pc så vi en modus der siktede først fikk nye venner som jente. Senere introduserte denne "jenta" mannen for vennene sine.

På grunn av reglene for datalagring hos teletilbyder(internettleverandører som Telenor, Canal Digital, NextGentel, m.fl.) visste vi at vi måtte jobbe raskt for å få ut relevant informasjon. Derfor

sendte vi kjapt en ny forespørsel til Microsoft, der vi etterspurte hvilke ip-adresser de 46 identene/e-postadressene hadde vært pålogget gjennom. Oversikten over disse ip-adressene gir informasjon om når e-postkontoen ble opprettet og alle tidspunkt der noen har vært logget på kontoen.

Hver gang noen logger seg på Internettet, får de tildelt ny ip-adresse fra teletilbyder, og hver gang noen logger seg på en e-postkonto registreres dette hos nettverten, f.eks. Microsoft, som er vert for bl.a. Windows Live Messenger. Vi mottok raskt svar på alle de 46 hos Microsoft, og fikk en oversikt over alle ip-adresser påloggingene hadde foregått gjennom.

Problemet oppsto da vi sendte alle Microsofts registrerte ip-adresser videre til teletilbyder. Teletilbyderne har bare anledning til å knytte ip-adressene direkte til en abonnent over en begrenset tidsperiode. Da vi tok kontakt med dem, kunne derfor bare 20 av de 46 e-postkontoene/identene spores tilbake til de eksakte abonnentene der noen hadde vært pålogget de aktuelle e-postkontoene. De andre ip-adressene var for gamle, siden e-postbrukeren ikke hadde vært på Internettet via MSN eller e-post de siste 21 dagene.

Det gikk relativt få dager fra vi startet etterforskningen av saken, frem til vi kontaktet teletilbyder for å få ut informasjon om hvilke abonnenter som har vært pålogget de aktuelle e-postkontoene. Det er så raskt som et lite politidistrikt som vårt er i stand til å jobbe frem denne typen informasjon. I vårt tilfelle førte dette til at vi måtte ta bort 26 ofre eller mulige ofre fra saken. Vi vet ikke om disse har møtt mannen, om de har vært utsatt for overgrep over Internettet, eller utsatt for andre straffbare handlinger. Vi vet ikke en gang hvem de er.

"Vår" sak viser hvor viktig det er at kriminalitet blir meldt inn raskest mulig, slik at politiet kan sikre spor, både med tanke på at skyldige ikke skal gå fri, og med tanke på at uskyldige ikke skal dømmes. Tidsrommet for datalagring skal ikke bare være til hjelp for fornærmede, men også for mistenkte." Vi kan dokumentere at siktede i denne saken har begått overgrep for mer enn 10 års siden gjennom beslag av filmmateriale.

Vi er i ettertid blitt møtt med at så lenge politiet sitter på opplysninger om e-post adresser så kan vi bare sende en mail for å oppnå kontakt, vi trenger ikke ip-adressene. Men det er ikke kurant for politiet å kun sende en mail for å oppnå kontakt med et mulig mindreårig offer, vi vet ikke hvem som ville leste den, hvordan eller om det blir reagert.

Vi er også fra ulike hold blitt møtt med at barn som er blitt utsatt for internettrelaterte overgrep bør få være i fred. Det trenger ikke å ha vært en ubehagelig opplevelse(for eksempel når en gutt tror han har kledd av seg foran en ung jente). Til det bemerkes det at vi ser jo at overgriperne ikke nøyer seg med kontakt på internett, men går videre til alvorligere overgrep. Det at en overgriper sitter på seksuelt relaterte bilder av barn er også et stort problem mtp spredning av bildematerialet, og den makt den kan gi en overgriper å sitte på disse bildene.

Denne saken og mange andre saker viser også at det er en enormt høy terskel for at barn som blir utsatt for overgrep selv avslører situasjonen. Vi er i stor grad avhengige av data som bevis.

Vi vil ikke bagatellisere frykten for et "overvåkningssamfunn", og behovet for et sterkt personvern. Men for oss som til daglig ser konsekvensene av kriminalitet blir for eksempel "ubehaget borgerne kan føle ved å vite at noen sitter med denne informasjonen" en mer "teoretisk trussel", enn de konsekvensene av alvorlig kriminalitet vi ser til daglig, de overgrepene vi faktisk har foran oss.

Det synes som om motstanderne av datalagringsdirektivet konsekvent bruker ordet overvåkning og dermed bidrar til at det oppstår misforståelser mht når politiet kan få tilgang til data og hva politiet vil få tilgang til. I gårsdagens lokalavis (Avisa Nordland) var det reportasje om motstandere som hadde stilt seg opp på posthuset og avkrevd kunder svar om hvem de sendte brev til og grunnlagt dette med at dette ville bli situasjonen (for elektronisk post) dersom datalagring iht EUS direktiv ble gjennomført.

Det synes som om motstanderne av datalagringsdirektivet ikke er villige til å diskutere konsekvensen av en situasjon der enkelte alvorlige straffbare handlinger i liten grad kan avdekkes og straffeforfølges, for eksempel internetrelaterte overgrep mot barn.

Det pekes på at politiet med dagens regelverk har tilstrekkelige metoder. Jeg klarer ikke å få tak i hvilke metoder man her mener kan gi samme nytten som tilgang til data.

Vi er først og fremst opptatt av Eus datalagringsdirektiv blir implementert og er inneforstått med at det må være strenge krav til informasjonssikkerhet og betydelige skranker mht når politiet får ut informasjonen.

Når det gjelder **hva som skal lagres** jf høringsnotatet s. 30 har vi ingen merknader til forslaget.

Det synes fornuftig å ikke skille **lagringstid** etter teknologi. Når det gjelder lagringstid finnes det jo en rekke eksempler på at etterforskning av grov kriminalitet kan ta lang tid, at forholdet meldes til politiet lenge etter at det har skjedd (typisk overgrep) slik at politiet vil kunne ha behov for data langt tilbake i tid.

Vi ser at momentet lagringstid er viktig i balansen mellom de ulike hensyn og bemerker at selv minstelagringstid i henhold til direktivet vil bety en betydelig forbedring og at man bør se hen til de øvrige land når man bestemmer hvor lang lagringstid man skal ha i Norge.

Når det gjelder utformingen av vilkår om **skjellig grunn til mistanke mot en bestemt person** så mener vi at det er svært uheldig at man for å få ut data må peke ut hvilken person som er mistenkt. Det må være tilstrekkelig at det er skjellig grunn til mistanke om at det har skjedd en bestemt straffbar handling av tilstrekkelig alvorlighet. Typisk vil være behovet for å finne ut hvem som kan knyttes til et åsted.

Det foreslås at utlevering av data bør kunne pålegges dersom det straffbare forholdet har en **strafferamme på mer enn 3 år**. Man må være klar over at det er en innskjerpelse i forhold til dagens mulighet til å få tilgang til den data som finnes. Det hadde vært ønskelig at domstolen hadde kunnet gjøre en skjønnsmessig vurdering av andre saker som "kan være særlig vanskelig å etterforske uten å kunne benytte data". Vi har ingen merknader til den oppregningen av slike lovbrudd som er gjort i pkt 4.12.

Det synes er riktig at domstolen skal fatte **beslutningen** om utlevering av data til politiet (primærkompetanse) og at Post og Teletilsynet dermed ikke gis noen rolle. Vi stiller imidlertid spørsmål om det er gjennomtenkt at påtalemyndigheten ikke gis hastekompetanse i akutte saker, for eksempel der man står ovenfor en alvorlig trussel. Det vises til at påtalemyndigheten er gitt hastekompetanse i langt mer inngripende metoder.

Med hilsen



Tone Vangen
politimester

Saksbehandler:

Tlf:



POLITIET

Politidirektoratet
Postboks 8051 Dep.
0031 OSLO

MOTTATT

26 MAR 2010

POLITIDIREKTORATET	
26 MARS 2010	
Arbeid	Arbeidsnr.
108-13	008
Saksnr.	Dokument
1060134	8

Deres referanse
2010/00134-2 008

Vår referanse
2009/01905-14 008

Dato
22.03.2010

Høring om datalagring

Innledning

Historiske data fra kommunikasjon er av avgjørende betydning for bekjempelse av alvorlig kriminalitet. I dagens situasjon bruker politiet slik informasjon for å avdekke den/de mistenktes bevegelser og kontakter/kontaktnett forut for og etter at straffbare handlinger er begått.

Vår oppfatning er at slike spor blir stadig viktigere i etterforskningen av alvorlig kriminalitet, og i stor grad avgjørende for å avdekke bakmenn. Fra vårt distrikt har vi flere eksempler på at trafikkdata fra telefoni har vært avgjørende for å avdekke nettverk innenfor narkotikainnførsel og -omsetning. Med trafikkdata har det vært mulig å avdekke hvem som deltar i kriminaliteten og hvilken rolle den enkelte har. For etterforskning av personer og miljøer som driver kriminalitet over et stort geografisk område har trafikkdata fra mobiltelefoni vist «ruta» og vært avgjørende for å knytte de mistenkte til en rekke straffbare handlinger. Urviklingen med en stadig økende gruppe mobile vinningskriminelle fra andre land viser at behovet for slike data vil øke. Vår erfaring er at vi ikke ville kunne avdekket kriminaliteten uten slike data.

Uten lagring av slike data i en periode, vil denne informasjonen være utilgjengelige for politiet. Registrering av slike data i sanntid, altså samtidig som kommunikasjonen finner sted, er bare mulig etter reglene om kommunikasjonskontroll. Ofte vil etterforskning av alvorlige enkelthandlinger eller etterforskning mot nettverk av kriminelle måtte baseres på å rekonstruere et sannsynlig hendelsesforløp. Den kriminelle handlingen, for eksempel et drap, distribusjon av overgrepssbilder av barn eller innførsel av narkotika, blir avdekket uten at politiet har forutgående kjennskap til at det skal skje. Da vil sanntids informasjonsinnhenting ikke gi noen informasjon om bevegelser og kontakter forut for handlingen. Det er da nødvendig å innhente slike data for å rekonstruere dette.

Telemark politidistrikt

Hva skal lagres

Vi er enige i forslagene til presisering av hva som skal lagres innenfor de ulike formene for kommunikasjon.

For fasttelefoni og mobiltelefoni foreslås det at stort sett den samme informasjonen som i dag skal lagres. I noen tilfeller vil det være relevant å hente ut trafikkdata knyttet til IMEI-nummer (selve mobiltelefonen) i stedet for eller i tillegg til IMSI-nummerne (telefonnumrene). Dette kan være aktuelt dersom brukeren av telefonen stadig bytter sim-kort i telefonen. I dag må dette innhentes som trafikkdata knyttet til det enkelte sim-kort.

For bredbåndstelefoni skal tilsvarende trafikkdata lagres. Vår oppfatning er at bredbåndstelefoni i stadig større grad vil bli brukt av kriminelle, ut fra en oppfatning om at sporene etter kommunikasjonen vil være vanskeligere tilgjengelig for politiet.

Lagringstid

Departementet beskriver på side 40 betydningen av at data lagres tilstrekkelig lenge til at de ikke forsvinner mens etterforskningen pågår.

Ved etterforskning av nettverk og kriminalitet som pågår over tid, vil nye mistenkte ofte «dukke opp» underveis i etterforskningen. Det krever at data er lagret slik at også etterforskningen av nye mistenkte kan bli rask og effektiv. Vår oppfatning er at 12 måneders lagringstid vil kunne være for lite i slike tilfeller.

Departementet påpeker den «nedkjølende effekten» automatisk lagring vil ha på den frie kommunikasjonen. Vi forutsetter at det etableres rutiner for sikker lagring av data der de lagres. Forslaget om et krav til skjellig grunn til mistanke og en rettslig behandling av spørsmålet om data skal behandles vil ha den konsekvens at politiet må begrunne for retten at det foreligger skjellig grunn til mistanke, noe som ikke er nødvendig i dagens ordning. Dette kravet bringer de aktuelle data inn i samme «system» som andre tvangsmidler mot mistenkte. I tillegg kreves det at de data det bes om utlevering av, er av slik betydning for etterforskningen at det ikke er uforholdsmessig at de utleveres. Det er etter vår oppfatning også et strengere krav enn det som ligger i dagens praksis.

Setter man disse strengere vilkårene opp mot lagringstiden og frykten for misbruk, er vår konklusjon at en lagringstid på to år ikke innebærer at politiet får muligheten til å drive «massiv kontroll» av befolkningen.

Bearbeiding av de innhentede data er en krevende prosess. Dette tilsier politiet ikke har ressurser til å innhente og bearbeide data som ikke er av avgjørende betydning for etterforskningen av alvorlig kriminalitet.

Den som med overveiende grad av sannsynlighet kan mistenkes for å være skyldig i alvorlig kriminalitet, har ingen beskyttelsesverdig interesse i at data om hans kommunikasjon slettes etter seks måneder eller ett år.

Etter vår oppfatning vil automatisk lagring i to år innebære at data i gitte tilfeller vil kunne være tilgjengelig gjennom hele etterforskningen av komplekse saker og i mange tilfeller gjennom behandling i tingrett og lagmannsrett.

I vurderingen av om politiet skal få tilgang til data for hele lagringstiden, vil det kunne settes opp strengere vilkår jo lenger bakover i lagringstiden man går. Det kan stilles tilleggsvilkår ved utlevering av data fra mer enn seks måneder eller ett år tilbake.

For de ulike typer telefoni er det etter vår oppfatning ikke noen grunn til å ha ulik lagringstid. Det samme gjelder for e-post, som i noen grad i denne sammenheng kan sammenlignes med tekstmeldinger på mobiltelefon.

For internettaksess har man ikke den samme logiske sammenheng med de øvrige data. Økende bruk av konvergerende kommunikasjonstjenester tilsier likevel at lagringstiden blir den samme også for internettaksess.

Hvilke lovbrudd skal begrunne utlevering?

Departementenes utgangspunkt med et krav til en strafferamme på 3 års fengsel eller mer synes godt begrunnet, og vil medføre at utlevering vil kunne skje ved etterforskning av de mer alvorlige forholdene. Vi er også enige i oppregningen av særlige bestemmelser som vil kunne begrunne utlevering.

Kravet om skjellig grunn til mistanke

Det vil i de aller fleste tilfellene innenfor dagens ordning foreligge skjellig grunn til mistanke mot brukeren av kommunikasjonsanlegget, og politiet argumenterer for dette i anmodningene om oppheving av taushetsplikten til Post- og teletilsynet. Innføringen av et slikt krav vil derfor bare i liten grad innebære noen begrensning for politiet, men vil sikre at begrunnelsen for en utleveringsbegjæring til retten er knyttet til bevis for en konkret mistanke mot en bestemt person.

I de tilfellene hvor det i dag innhentes data fra basestasjoner, vil politiet få informasjon om et stort antall personers bruk av mobiltelefon innenfor basestasjonens dekningsområde. I disse tilfellene er det ofte slik at det er åpenbart at en straffbar handling er begått, men at mistanken enda ikke kan knyttes til en bestemt person. Det må være anledning til å innhente slike data også i framtiden, og kravet til skjellig grunn til mistanke må ikke stenge for dette spesielle tilfellet.

Med hilsen





POLITIET

MOTTATT

25 MAR 2010

Politidirektoratet
Pb 8051 Dep
0031 Oslo

POLITIDIREKTORATET	
25 MARS 2010 3	
Arkiv: A08-13	Adressat: 008
Saksnr: 10/00134	Dokument: 007

Deres referanse
2010/00134-2 008

Vår referanse
201000358

Dato
22.03.2010

Uttalelse fra Haugaland og Sunnhordland politidistrikt (HSPD) om forslaget til implementering av datalagringsdirektivet

Det vises til Politidirektoratets brev av 22. februar 2010 hvor det bes om politidistriktets uttalelse om ovennevnte.

HSPD anser datalagring som et svært nyttig verktøy i kampen for å oppklare straffbare forhold. Distriktet har også det siste året nyttiggjort oss de spor trafikkdata har gitt i etterforskningen av vinnings- og narkotikasaker. Behovet for trafikkdata synes særlig å være rettet inn mot å belyse siktedes bevegelsesmønster og kontaktnett. To av de mest omfattende straffesakene i distriktet tas her med som eksempler:

1. Lervik ur

En urmaker i Haugesund sentrum ble i juli 2009 utsatt for grovt tyveri. Verdier for flere millioner ble stjålet. Gjerningsmennene benyttet flere stjålne biler under tyveriet, den ene som rambukk. Fire personer fra Polen ble noe tid etter pågrepet og senere dømt i tingretten. Innhentet trafikkdata viste hvilke sim-kort (med tilhørende telefonnummer) som hadde blitt benyttet i den enkeltes mobiltelefon. Trafikkdata viste videre hvor den enkelte siktedes mobiltelefon hadde befunnet seg. Dette medførte at en kunne knytte dem opp til aktuelle steder samme dato som det ble utført grove tyverier i Haugesund og senere i Stavanger.

I Stavanger var det ikke tekniske spor som kunne knytte dem til åstedet. Trafikkdata og registrerte bompasseringer gjorde at en kunne knytte gjerningsmennene til Egersund, hvor tyveri av bilen som ble brukt som rambukk fant sted, og til Stavanger hvor åstedet for det grove tyveriet var. Bompasseringer eller trafikkdata ville alene neppe vært tilstrekkelig som bevis, men i fellesskap bidro dette materialet til å synliggjøre bevegelsesmønsteret til gjerningsmennene.

2. Narkotika

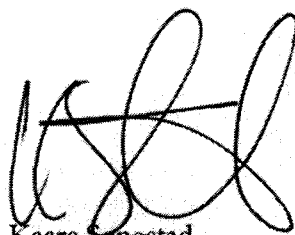
En av de større narkotikasaker vi har hatt i distriktet var mot en irakisk statsborger med fast bosted i Norge. Han tilstod å ha kjøpt og fraktet narkotika til Haugesund ved to

Haugaland og Sunnhordland politidistrikt

etterforskningen.

Andre myndigheters tilgang til data

Forslaget om domstolsbehandling synes ikke å omfatte Kredittsynets tilgang til trafikkdata. HSPD mener at Kredittsynet av hensyn til kriminalitetsbekjempelsen, bør gis tilgang til de samme trafikkdata som det politi/påtalemyndighet får. Det naturlige synes da at Kredittsynet undergis de samme vilkår for tilegnelsen. Derfor foreslås det å innføre domstolsbehandling også for Kredittsynet tilgang til trafikkdata.



Kaare Songstad

Saksbehandler:

Padv Bjarne Myklebust

Tlf:

52868128



POLITIET

Politidirektoratet
Att: Bente Storruste
Postboks 8051 Dep
0031 OSLO
Norge

Dens referanse
2010/00134-2 008

Vår referanse
2010/00584-2 053

Dato
09.04.2010

Høring om datalagring

Generelt gir en implementering av datalagringsdirektivet en gevinst da det forenkler etterforskning av alvorlig kriminalitet, samtidig styrkes den enkelte borgers rettsikkerhet i form av at elektroniske spor som kan bevise skyld/uskyld også tilgjengeliggjøres i en lengre periode enn tidligere.

Elektroniske spor i saker som for eksempel omhandler narkotika, sedelighet m.flere forholder seg i dag ikke til landegrensene. Det å tilpasse seg til et felles regelverk via datalagringsdirektivet vil gjøre det enklere å samarbeide internasjonalt med å oppklare slike alvorlige saker.

1. I forhold til hva som eventuelt skal lagres

På telefonisiden er oppstillingen i pkt 4.4.1, 4.4.2, 4.4.3 utfyllende. Når det gjelder internettaksess er oppstillingen i pkt 4.4.4 utfyllende.

2. Lagringstid og teknologi

Vi er enige i at det er en fordel å ikke skille lagringstid i forhold til hvilken teknologi som benyttes. Vi er derimot uenig i at lagringstiden settes til 6 måneder. Både Finland og Danmark har satt lagringstid til 1 år. Det bør Norge også gjøre. Det at Sverige ikke har implementert datalagringsdirektivet ser ikke vi kan benyttes som argument for å ha en kortere lagringstid enn de andre nordiske landene.

Vi mener videre at når det er retten som begjærer innsyn, så er personvernet sikret. Vi ser det også som en fordel at det ikke er behov for at Post- og teletilsynet fritar tilbyder fra taushetsplikten i de saker som retten har begjært innsyn. Dette fordi vi sparer tid i initialfasen av alvorlige straffesaker.

3. Oppstillingen av lovbrudd som alternativ til fengsel i 3 år eller mer

Alternativene som er opplistet på side 47 og 48 ser grei ut.

Nordmøre og Romsdal politidistrikt

Administrativ enhet, besøk: Storgata 43
Post: Postboks 244, 6501 KRISTIANSUND
Tlf: 71 58 90 00 Faks: 71 67 30 99
E-post: post.noro@politiet.no

Org. nr.: 983 998 585
Bankgiro: 7694.05.11573

4. Vilkåret om skjellig grunn til mistanke

Kravet om at politiet må godtgjøre at "noen med skjellig grunn mistenkes" høres fornuftig ut. Dette er i henhold til rutiner politidistriktet benytter i dag.

5. Videreføre delt tilsynsansvar mellom Post- og teletilsynet og Datatilsynet

Dette fungerer bra i dag.

6. Andre myndigheters tilgang til data

Det vil være unaturlig om andre enn politiet skal få tilgang til trafikkdata uten at det er en straffesak, og dermed uten at retten ber om å få trafikkdata utlevert. Hvorfor skal andre myndigheter få tilgang til disse dataene på en enklere måte enn politiet?

7. Innhenting av data for å avdekke pressens kilder

Kildevernet bør opprettholdes. Men det må ikke strekkes så langt at politiet får forbud mot å etterforske en person fordi han/hun har tipset pressen om egne straffbare forbrytelser.

Med hilsen

Rune Nordvik
IKT-etterforsker

Saksbehandler:
Rune Nordvik
Tlf: 71589501



POLITIET

Politidirektoratet
Pb 8051 dep.
0031 Oslo

Deres referanse
20100134

Vår referanse
201001499

Dato
26.03.2010

(anonymisert)

Høring – datalagring

1. Innledning

Mandatet til høringsuttalelsen er angitt i høringsbrev fra Politidirektoratet av 22. februar 2010, med videre henvisninger til høringsbrev fra samferdselsdepartementet av 8. januar 2010.

Det vil først bli gitt et sammendrag av konkrete saker hvor viktigheten av teledata for politiets arbeid med alvorlig kriminalitet belyses (punkt 2). Eksempelene er hentet fra spesialavsnittene ved Oslo politidistrikt. Det understrekes imidlertid at teledata utgjør et sentralt bevis i svært mange saker som etterforskes ved Oslo politidistrikt. Deretter behandles de problemstillingene som er fremhevet i høringsnotatet (punkt 3). Avslutningsvis er det inntatt noen generelle merknader som er innkommet fra hvert spesialavsnitt (punkt 4).

Oslo politidistrikts høringssvar følger denne kronologien:

1. Innledning.....	1
2. Konkrete eksempler.....	2
2.1 Eksempler fra etterforskning og påtale ved seksjon for organisert kriminalitet	2
2.1.1 Operasjon Abuelo.....	2
2.1.2 Operasjon Turowa	3
2.1.3 Operasjon Outback	3
2.1.4 Operasjon Ulven.....	4
2.1.5 Operasjon Shampoo.....	4
2.2 Eksempler fra Analyse ved seksjon for organisert kriminalitet	5
2.2.1 Operasjon Tystnad.....	5
Operasjon Laban.....	5
2.3 Eksempler fra seksjon Vold og Sedelighet.....	6
2.3.1 Dobbeltdrap i Bjerregaardsgata – avgjørende bevis.....	6
2.3.2 Drap i Maria Dæhliesvei.	6
2.3.3 Frihetsberøvelse og trussel mot fengselsbetjent.....	6

Oslo politidistrikt

91 Strategisk Stab, besøk: Grønlandsleiret 44, 0190 OSLO
Post: Postboks 8101 Dep, 0032 OSLO
Tlf: 22 66 90 50 Faks: 22 66 87 01

Org. nr.: 961398142
Postgiro: 7694.05.08319

2.3.4 Ny domfellelse for medvirkning i samme sak.....	6
2.3.5 Drap på Haugerud (behov for lengre lagringstid)	7
2.3.6 Nordahl Brunsgate (behov for lengre lagringstid).....	7
2.3.7 Grovt overfall og voldtektsforsøk natt til 16.9.06– Trosterud T-banestasjon..	7
2.3.8 Anmeldelse på bortføring, neddoping, fysisk vold og grov voldtekt - pirattaxi.	7
2.3.9 Falsk anklage – grov voldtekt.....	8
2.3.10 Gruppevoldtekt av somalisk jente i januar 2007, flere domfelte.....	8
2.4 Eksempler fra Finans og Miljøseksjonen	9
2.4.1 Sak fra bygg og anleggsbransjen.....	9
2.4.2 Operasjon Lefdal	9
2.4.3 Operasjon Plastic Fantastic.....	10
3 Bemerkninger til problemstillinger som er fremhevet i høringsnotatet	10
3.1 Generelle synspunkter	10
3.2 Hvilke typer data bør lagres?.....	11
3.3 Lagringstid og forslaget om ikke å skille lagringstid etter teknologi.....	11
3.4 Oppregningen av lovbrudd som alternativer til strafferammekravet	12
3.5 Forslag om at kun retten skal kunne pålegge besitteren å utlevere data	12
3.6 Utformingen av vilkåret for skjellig grunn til mistanke.....	13
4. Generelle synspunkter fra avdelingene	13
4.1 Synspunkter fra etterforskning og påtale ved seksjon Organisert Kriminalitet	13
4.2 Generelle synspunkter fra Analyse ved seksjon for Organisert Kriminalitet.....	13
4.3 Generelle synspunkter fra seksjon Vold og sedelighet.....	14
4.4 Generelle synspunkter fra seksjon for Finans og miljø.....	15

2. Konkrete eksempler

I dette avsnittet er det oppsummert noen konkrete saker som er etterforsket hvor trafikkdata har hatt stor bevismessig betydning for tiltale, dom eller henleggelse, og/eller hvor mangelen på trafikkdata har hatt stor betydning for etterforskningen og sakens utfall, og hvor lengre lagringstid ville gitt mulighet for oppklaring av saken

2.1 Eksempler fra etterforskning og påtale ved seksjon for organisert kriminalitet

2.1.1 Operasjon Abuelo

I oktober 2008 ble to unge jenter pågrepet på Arlanda med 6,2 kg kokain. Svensk etterforskning viste at stoffet var hentet i Brasil og var på vei til Oslo. Det var konkret informasjon som pekte mot et norsk bakmannsapparat. Norsk politi overtok etterforskningen og iverksatte en omfattende operasjon mot bakmannsapparatet. På dette tidspunktet ble det innhentet teledata for oktober, noe som gav direkte bevis mot to personer i Norge. Dette var personer som var i direkte kontakt med kurerene, og konfrontert med dette erkjente de forholdet. I denne saken ble tre personer dømt til henholdsvis 5, 6 og 7 års fengsel i januar 2010.

Gjennom etterforskningen ble det våren 2009 avdekket at bakmannsapparatet hadde foretatt flere innsmuglinger av kokain i løpet av 2008. Dette ble avdekket gjennom avhør, valutatransaksjoner samt gjennomgang av beslaglagte gjenstander. På samme måte som teledata gav avgjørende bevis mot bakmenn i ”Arlanda-saken”, ville teledata vært verdifulle bevis i forbindelse med innførslene foretatt tidligere i 2008. Da disse smuglerturene ble

avdekket var det gått over seks måneder siden forholdet var begått, og dermed ikke mulig å innhente teledata. Disse sakene er fremdeles under etterforskning.

Saken omfatter totalt 20 siktede personer som er knyttet direkte til narkotikainnførsler. I tillegg er 13 personer siktet for valutatransaksjoner som er knyttet til kokainsmugling.

2.1.2 Operasjon Turomva

Tre personer ble i februar 2009 pågrepet for oppbevaring av 1,6 kilo heroin. Person A kom fra Tyrkia via Sverige til Norge med den beslaglagte narkotikaen i sekken. Det var forutgående kommunikasjonskontroll i utlandet, slik at myndighetene i Sverige og Norge visste når og hvor person A ville komme. Det var spaning på person A, og politiet observerte to personer (B og C) som møtte person A i Oslo. Politiet fulgte de tre personene og observerte at person A overga sekken til person C før alle tre ble pågrepet.

Person A fortalte i avhør at han var sendt til Sverige av noen personer i Tyrkia for å jobbe og kjente ikke til noe narkotika. Person A og B nektet også ethvert kjennskap til den beslaglagte narkotikaen. Selv om person B og C var observert sammen nektet person B for at han kjente noe særlig til person C, og overhodet ikke noe kjennskap til person A. Person A fortalte etter hvert i avhør av hvem (bakmenn) han ble sendt til Sverige/Norge for å jobbe, og han oppga deres telefonnumre. Person A erkjente i avhør senere at han visste at det var narkotika i sekken han hadde med (hasj, ikke heroin).

Teletrafikk i saken avdekket at det hadde vært kontakt mellom person B og C med bakkemennene i Tyrkia. Spesielt var det utstrakt kontakt mellom person B og bakkemennene i Tyrkia, noe som ble et viktig bevis i tingretten.

I februar 2010 ble det avsagt dom og retten la vekt på både politiets observasjoner og teletrafikken i saken. Teletrafikken knyttet både person B og C til bakkemenn i Tyrkia, og retten la til grunn at person B hadde hatt en organisatorisk rolle i mottaket av heroinet på bakgrunn av teletrafikken. A idømt 6, 6 års fengsel, B idømt 9 års fengsel, for å ha organisert mottaket samt for narkotikaheleri av 500 000,-, og C ble idømt 7 års fengsel. Dommen er ikke rettskraftig og er anket av de domfelte.

Selv om politiet hadde gode observasjoner av de tre tiltalte, var teletrafikken et sentralt bevis. Teletrafikken knyttet de to mottagerne til bakkemennene til hverandre og synliggjorde deres roller.

2.1.3 Operasjon Outback

I en narkotikasak ble det i august 2006 beslaglagt 26 kg amfetamin hjemme hos siktede (A). A valgte i politiavhør å fortelle om oppdragsgiver/bakmann (B) og personen som innførte amfetaminet til Norge (C) og overleverte det til A. A oppbevarte og leverte ut store kvantum narkotikaen for B. Tiltalen omfattet totalt 108 kg amfetamin. A oppbevarte narkotikaen sammen med D. På bakgrunn av As forklaring ble B, C og D pågrepet. Alle de tre nektet ethvert kjennskap til narkotikaen. Et sentralt bevistema var å kontrollere troverdigheten i As forklaring. På dette punktet var trafikkdata et helt avgjørende bevis.

Ved gjennomgang av trafikkdata i saken viste det seg at As forklaring om hvor han hadde vært til ulike tidspunkter, hvilke rute han hadde kjørt og tidspunkter for overlevering av narkotikapartiet stemte overens med trafikkdata. Videre var det utstrakt bruk av telefonkiosker i saken, da B var redd for avlytting av sin mobiltelefon. Dette var

opplysninger som A kom med i politiforklaringer. På dette punktet viste også trafikkdata at A sine forklaringer stemte, idet det var unormalt stor bruk av telefonkiosker. Videre svekket funn i trafikkdata troverdigheten til B ved at hans politiforklaringer ikke stemte med faktiske funn i trafikkdata. Dette var i hovedsak knyttet opp til hvor han befant seg på ulike tidspunkter (basestasjoner).

B, C og D forklarte at de ikke hadde noen kjennskap til hverandre. Trafikkdata i saken knyttet de tre til hverandre på sentrale tidspunkt i saken. Funn i teledata knyttet til D underbygde As forklaring om at han hadde vært i kontakt med involverte i saken.

Tingretten og lagmannsretten legger i sine dommer stor vekt på funnene i trafikkdata, hvor de finner domfelte As forklaring er troverdig, som igjen medførte at han også ble trodd på andre punkter. I dom fra Borgarting lagmannsrett januar 2010 ble A idømt 6, 5 års fengsel inkl 50% strafferabatt, B idømt 16 års fengsel og inndragning på 9 millioner kroner. Inndragningsbeløpet knytter seg til at retten også dømte B for heleri, og fant det bevist at han over lang tid har opparbeidet seg verdier (hus, bil m.m.) som er utbytte av straffbar virksomhet. Videre ble C idømt 10 års fengsel, og D idømt 12 års fengsel.

Selve innførselen av 108 kg amfetamin skjedde i april 2006. Etterforskningen i saken startet med beslag av 26 kg i august 2006. I tiden mellom innførsel og beslag ble resten av amfetaminet solgt.

Etter hvert som etterforskningen, herunder politiavhør og analyser basert på innhentet teledata, avdekket stadig flere involverte, ble det relevant å innhente teledata for nye telefonnummer. Blant annet ble C først identifisert senere på høsten. På dette tidspunktet var det for sent å innhente teledata for tidspunktet han hadde innført narkotikaen til Norge. Slik teledata ville kunne avdekke flere involverte. Det kunne gitt viktig informasjon om leverandørledd i Nederland og andre involverte i Norge i tillegg til å belyse hans egen rolle.

2.1.4 Operasjon Ulven

En kvinne anmeldte en person for voldtekt. Forholdene fant sted i juli og august. Hun viste seg å jobbe som prostituert for personen som har voldtatt henne. Etterforskningen viste at hun har arbeidet på "strøket" sammen med en annen kvinne. Denne kvinnen hadde flyttet til Litauen og ble avhørt der i november. Norsk politi mottok avhøret i desember. Kvinnen fortalte at hun arbeidet for samme person, og at han også har voldtatt henne. Hun forklarte videre at hun alltid sendte tekstmeldinger før og etter at hun møtte kunder. Hun var følgelig også et offer, hvor teledata ville underbygget hennes forklaring – dersom den ikke var slettet.

Bakgrunnen for at anmeldelsene kommer lang tid etter gjerningstidspunktet i disse sakene, er at kvinnene får en refleksjonsperiode. De blir oppfordret til å tenke seg om, og tiden vil automatisk løpe.

2.1.5 Operasjon Shampoo

I en narkotikasak ble det i november 2007 beslaglagt cirka 10 kg heroin i bilen til to personer (A og B) på grensen mellom Nederland og Tyskland. A valgte i politiavhør å fortelle om to oppdragsgivere/bakmenn (C og D). Person B valgte i utgangspunktet ikke å forklare seg. A hadde ikke spesifikke navn eller ID på C og D, men viste til telefonsamtaler han hadde hatt med disse før A og B reiste til Nederland, samt samtaler mens de to var i Nederland og hentet heroinet.

På bakgrunn av As forklaring ble det iverksatt etterforskning mot person C og D. Det var i initialfasen innhentet trafikkdata på samtlige involverte personer.

Person C og D ble pågrepet og avhørt. De nektet ethvert kjennskap til narkotikaen og forsøk på innførsel til Norge av dette. Et sentralt bevistema var å kontrollere troverdigheten i As forklaring. På dette punktet var trafikkdata et helt avgjørende bevis. Ved gjennomgang av trafikkdata i saken viste det seg at det A forklarte i avhør omkring kommunikasjon med C og D stemte overens med trafikkdata. A sin forklaring omkring reiserute ble også kontrollert opp mot basestasjoner, for å styrke hans forklaring på denne måten. Person C forklarte at han ikke hadde noen kjennskap, eller hadde hatt telefonisk kontakt med A eller B. Trafikkdata i saken viste imidlertid at C hadde hatt utstrakt telefonisk kontakt med A og B. Person D forklarte at han kun hadde hatt sporadiske samtaler til person A og B. Funn i teledata viste imidlertid at person D hadde hatt utstrakt kontakt med både person A og B. Etter konfrontasjon med disse opplysningene valgte person D å erkjenne å ha videreformidlet oppdraget med å hente heroinet i Nederland. Han ønsker imidlertid ikke å gi opplysninger om person C sin tilknytning til saken. Person C nekter fremdeles å ha noe med saken å gjøre.

Saken er oversendt Statsadvokaten i Oslo, og det forventes hovedforhandling i løpet av andre halvdel av 2010.

Kripos hadde i initialfasen innhentet teledata i saken, som ble oversendt Oslo pd.i 2009. Dersom Kripos ikke hadde innhentet teledata i initialfasen hadde det vært meget vanskelig å tiltale person C og D.

2.2 Eksempler fra Analyse ved seksjon for organisert kriminalitet

2.2.1 Operasjon Tystnad

Kommunikasjonskontroll avdekket en innførsel av større mengder narkotika 15. november 2007. Person 3 og 4 var kurerer, kommunikasjonskontroll/spaning/pågrep viste at person 1 var hovedmottager. Person 2 var syk denne dagen, og han var ikke tilstede da overleveringen av varene fant sted. Politiet klarte derfor ikke å bevise at han hadde en rolle i dette. Trafikkdata viste derimot samsvarende mønster på basestasjonene til person 1 og 2 to uker forut for denne innførselen, 6. november, som tydet på at det også denne dato hadde foregått en innførsel. Ved innhenting av trafikkdata på den ene kurertelefonen viste også denne innslag i Norge/Oslo 6. november. Ytterligere forklaringer og opplysninger gjorde at man fikk dømt de siktede også for denne innførselen. Ved en feiltagelse ble det ikke innhentet trafikkdata på et av telefonnumrene til person 2 ved tilslag. Da det senere viste seg at dette var svært nødvendig, var dette materialet gått tapt p.g.a lagringstid. Gjennomgang av trafikkdata viste også at person 2 daglig frekventerte en basestasjon et stykke fra hans egen bopel. Dette viste seg å være depotleiligheten der stoffet ble oppbevart, pakket og veid. Tre personer ble alle dømt til 5-6 års fengsel.

Som en oppsummering var innhenting, bearbeiding av trafikkdata av avgjørende betydning for å finne den første innførselen, samt depotleiligheten.

Operasjon Laban

Kommunikasjonskontroll avdekket overlevering av to kg heroin og at det fantes mer. I etterkant av tilslaget ble depotet funnet, hvor det ble beslaglagt ca. 17 kg heroin. Trafikkdata på hovedpersonene viste seg å være viktig, idet ikke alle personene inngikk i

kommunikasjonskontrollen. Trafikkdata viste knytningene mellom de ulike personene hadde med hverandre. Basestasjonene viste at "løpegutten" ved flere anledninger hadde vært på basestasjonen som dekket adressen for depotet.

De tre domfelte fikk fengselsstraffer på hhv. 15 år og seks måneder, 11 år og åtte år.

2.3 Eksempler fra seksjon Vold og Sedelighet

2.3.1 Dobbeltdrap i Bjerregaardsgata – avgjørende bevis

To studenter ble funnet drept på sin felles hybel i Bjerregaardsgata, fredag 20. februar 2004. Det var siktede selv som varslet vaktmester om at han ville inn på hybelen for å sjekke om de var der.

Teledata var et sentralt og avgjørende bevis i saken. Siktede sendte en tekstmelding fra en av de fornærmedes telefoner til sin egen telefon etter at de var drept. Undersøkelser hos teleselskapet NetCom viste at simkortet til en av de fornærmedes telefoner har stått i siktede sin telefon ved minst to anledninger.

2.3.2 Drap i Maria Dabliesvei

En person ble funnet drept 29. januar 2009. Flere opplysninger i saken peker mot at drapet fant sted 26.01.09, på kvelden. Trafikkdata fra fornærmede og siktedes telefon viste at de hadde en felles kontakt drapsdagen og vi kunne ut fra siktedes basestasjoner se at han oppholdt seg på drapsstedet da fornærmede ble drept.

2.3.3 Frihetsberøvelse og trussel mot fengselsbetjent

Rømning under permisjon fra fengsel 7. juli 2006. Tre personer ble domfelt for trusler og frihetsberøvelse mot fengselsansatte til ubetinget fengsel fra 2 ½ til 3 ½ år. Teledata og bompassering var sentrale bevis under etterforskningen og under hovedforhandling. To av de domfelte var brødre (én av dem fangen som rømte), tredjemann en bekjent av begge. Bompassering og basestasjon var sentralt mot tredjemann, som viste hans bevegelser i det sentrale tidsrom. Teledata var enda mer sentralt mot broren som medvirket, idet han var i kontakt med tredjemann få minutter før hendelsen, og i tillegg i et mistenkelig omfang dagen og ukene i forveien. Uten teledata ville bevisbildet vært problematisk, og helt sikkert ført til henleggelse uten tiltale mot broren som medvirket.

Videre var det kun politiets aktive innsats i den innledende fase som sikret disse teledata, idet det gikk flere måneder før den første ble pågrepet (fangen rømte til Tyskland). Hvis man ikke hadde sikret teledata i forkant av pågripelsen, ville man risikert at dataene ikke lenger var tilgjengelig. Dommen kan leses i Lovdata med ref LB-2008-105706 og Rt-2009-435.

2.3.4 Ny domfellelse for medvirkning i samme sak

Fjerde person senere dømt for medvirkning i samme sak som nevnt under punkt 2.3.3. Tiltalen ble skjerpet til legemsbeskadigelse med betydelig skadefølge, idet de fornærmede ble langvarig sykemeldt og ute av stand til å fortsette i yrket. Også her var teledata sentralt. Basestasjon og telefonkontakt med tredjemann (som nevnt over) kort tid før hendelsen. Uten teledata ville det neppe vært grunnlag for tiltale eller dom.

Fjerdemann ble pågrepet nesten to år etter hendelsen. Uten sikring av teledata i den innledende fasen av etterforskningen, ville disse opplysningene ikke vært tilgjengelige ved pågripelsen.

2.3.5 Drap på Hangerud (behov for lengre lagringstid)

Drap der siktede etter drapet forsøkte å skjule spor ved å tenne på en bil med offeret i.

Etterforskningen har avdekket at det sannsynligvis er et bestillingsdrap. Det tok tid før politiet fant en link mellom siktede og den han drepte på oppdrag fra, og mye trafikkdata var da gått tapt. Flere av de personene politiet jobber med opererer med flere telefonnummer og det kan gå tid før vi får vite hvilke telefonnummer som er brukt. Tre mnd kan da være alt for kort tid. Mye trafikkdata går tapt på den tiden.

2.3.6 Nordahl Brunsgate (behov for lengre lagringstid)

En person ble funnet drept i Nordahl Brunsgate. Saken står fortsatt med ukjent gjerningsmann. Vi har i dag opplysninger som kunne blitt avkreftet eller bekreftet dersom trafikkdata hadde blitt lagret i en lengre periode.

2.3.7 Grovt overfall og voldtektsforsøk natt til 16.9.06– Trosterud T-banestasjon

Fornærmede fikk brudd i pannen som følge av vold benyttet mot henne under overgrepet. Forsøket ble avsluttet på grunn av utenforstående som ropte til domfelte, som forsvant fra stedet. Siktede ble først dømt – OT 20.6.08 (anket 26.9.08), deretter frikjent i Borgarting lagmannsrett (BL) 26.9.08 - dom ble satt til side, deretter dømt igjen – BL 22.6.09.

Sentralt bevis under etterforskningen var bompassering og teledata. Domfelte var tidligere ustraffet sønn av en politimann, avtjente på den tiden verneplikt og forsøkte seg på opptak i Telemarksbataljonen. Domfelte forklarte seg uriktig hele veien og endret og tilpasset sine forklaringer etter hvert som han ble konfrontert med bevis for at han løy. I tillegg til først å ha nektet for å ha befunnet seg i det aktuelle området i det hele tatt, forsøkte han også å mistenkeliggjøre en delvis navngitt bekjent og forklarte at han lånte bilen mens domfelte sov. DNA-prøver fra fornærmede og senere undersøkelser i domfeltes bil ga ingen relevante funn. Bompassering og basestasjonsinnslag var helt sentralt for å få plassert domfelte i umiddelbar nærhet til åstedet på tidspunkt som samsvarte med overfallet. Hans passering av bomringen i Tvetenveien med egen bil (i umiddelbar nærhet til åstedet) sammenholdt med utskrift av hans trafikkdata og mobiltelefonbruk i det aktuelle tidsrommet, gjorde at politiet kunne utelate at andre enn domfelte selv hadde kjørt bilen, og at han samtidig hadde befunnet seg i området for overgrepet. I løpet av natten og like etter overgrepet, kontaktet domfelte to kamerater både med SMS og oppringning hvor han ba dem om å gi han alibi ved å si at han hadde vært hos dem den aktuelle natten – ”hvis politiet tok kontakt med dem”. Denne oppfordringen ble gjentatt pr. SMS til den ene av kameratene under en pause i et senere politiavhør. Uten teledata og tilgang til bompasseringen, ville bevisbildet vært problematisk og høyst sannsynlig ført til henleggelse med ukjent gjerningsmann - eventuelt ført til frifinnelse.

2.3.8 Anmeldelse på bortføring, neddoping, vold og grov voldtekt - pirattaxi.

Den fornærmede kvinnen skal ha blitt dopet ned ved bruk av sprøyter, lagt i bagasjerommet på bilen, kjørt til ukjent sted hvor hun ble voldtatt på det groveste av flere gjerningsmenn. Etter voldtekten ble hun igjen puttet i bagasjerommet, transportert tilbake, kastet ut og etterlatt på gaten.

Politiet undersøker om kvinnen har fremsatt påstandene om bortføring, neddoping og senere voldtekt – for å skjule et annet forhold for sin samboer. Den "andre" parten har

forklart at det var SMS-kontakt mellom han og kvinnen. Politiet har grunn til å tro at kvinnen har forklart seg uriktig, unøyaktig og har tilpasset sine forklaringer etter hvert som hun har blitt konfrontert med bevis i saken. Hun har også flere ganger endret mulig sted for overgrepet – med et stort geografisk spenn. Innslag på trafikkdata og basestasjoner gir oss et helt klart bilde av hvor hun har beveget seg i Oslo sentrum på aktuelt tidsrom – de er ikke sammenfallende med hennes øvrige forklaring på hvor hun har vært og til hvilket tidspunkt hun har vært på de forskjellige stedene.

Ut ifra trafikkdata i denne saken – sammenholdt med hennes og vitners forklaringer – fremstår det som åpenbart at hennes anmeldelse ikke er reell. Da det kreves omfattende sannsynliggjøring og bevis for å skulle ”snu” en anmeldelse, vil opplysningene fra innhentet trafikkdata i denne saken være helt avgjørende for om hvorvidt dette vil gjøres eller ikke. Trafikkdata har dermed også vært avgjørende for å sikre at uskyldige ikke blir tiltalt eller dømt.

2.3.9 Falsk anklage – grov voldtekt

Fornærmede innga opprinnelig anmeldelse på voldtekt, i forbindelse med at hun kom til Oslo og skulle møte en venninne. Venninnen dukket ikke opp. Av anmeldelsen fremgikk at kvinnen utenfor en bygård ble oppsøkt av to menn, de truet henne inn i en leilighet hvor hun ble voldtatt på det groveste av den ene av mennene etter at den andre hadde forlatt leiligheten. Hun ble i tillegg påtvunget et hvitt pulver. Kvinnen ga en beskrivelse av gjerningspersonen og identifiserte leiligheten hvor voldtekten skulle ha skjedd, og hun opprettholdt forklaringen i nytt politiavhør noen dager senere. Hennes opplysninger førte til at politiet rykket ut til den påviste leiligheten hvor den anmeldte mannen befant seg sammen med sin kone og to barn. Hans kone og barn måtte forlate leiligheten sent på kvelden for at politiet skulle gjøre tekniske undersøkelser. Mannen ble pågrepet og siktet for voldtekt. I avhør fortalte mannen at han hadde hatt sex med domfelte, men at det hele var avtalt og helt frivillig. Han forklarte at de hadde vært i kontakt flere ganger og over lang tid både via en chattekanal på mobiltelefon og senere direkte pr. SMS til hverandres telefoner. Kvinnen hevdet på sin side at hun ikke visste hvem voldtektsmannen var. Da hun ble konfrontert med meldingene som mannen hadde tatt vare på, samt at politiet hadde innhentet teledata i saken, fastholdt hun likevel sin forklaring, og forklarte meldingene med at noen måtte ha sendt dem mens hun lå og sov. I politiets innhentede trafikkdata fra fem mnd tilbake i tid, viste det seg at det var mer enn 200 registrerte SMS mellom kvinnen og mannen. Kvinnen ble domfelt for falsk anklage i Oslo tingrett den 10. mars 2009.

I dette tilfellet var det helt avgjørende for saken og den endelige dommen at mannen på eget initiativ hadde tatt vare på meldingene fra kvinnen, samt at innhentet trafikkdata viste at fornærmedes forklaring stemte i forhold til langvarig og hyppig kontakt – og dermed at anklagen var falsk.

I motsatt tilfelle – dersom vi ikke hadde hatt tilgang til trafikkdata – er det en åpenbar fare for at mannen kunne ha blitt urettmessig dømt for en voldtekt han ikke hadde begått.

2.3.10 Gruppevoldtekt av somalisk jente i januar 2007, flere domfelte

I løpet av etterforskningen ble det forsøkt å innhente trafikkdata på fornærmede i tidsrommet hvor hun ble utsatt for gruppevoldtekt. Pga uheldige omstendigheter ble trafikkdata ikke sikret før det hadde gått for lang tid. Forsvarerbenken kritiserte sterkt etterforskningen fordi de mente at fornærmedes trafikkdata ville ha vist at hun hadde hyppig kontakt med andre – på tidspunkt hvor hun selv hadde forklart at hun ble voldtatt og var

borttatt sin telefon. De tiltalte i saken mente at hun hadde snakket med andre jenter på ”festen” og invitert dem med opp dit. Dersom trafikkdata hadde vært lagret lenger og dermed kunne rullet å bli sikret, hadde dette blitt avklart.

Tre av de siktede ble domfelt i Borgarting lagmannsrett i juni 2008. Den fjerde av de siktede ble først domfelt i Oslo tingrett i januar 2008, men deretter frikjent i Borgarting lagmannsrett i juni 2008 hvor dommen ble satt til side. Han ble imidlertid domfelt i Borgarting lagmannsrett i oktober 2008. Femte og sistemann ble først domfelt for medvirkning i Oslo tingrett i januar 2008, men ble frikjent i Borgarting lagmannsrett i juni 2008.

2.4 Eksempler fra Finans og Miljøseksjonen

I det følgende gis tre eksempler på hvordan dagens ordning på den ene siden har gitt oss redusert mulighet til å trygge en god rettssikkerhetsmessig prosess for de involverte i en sak, samt på den andre siden hvilket utbytte trafikkdata har gitt i de tilfellene vi har vært i besittelse av historikk som dekker gjerningstidspunktet.

2.4.1 Sak fra bygg og anleggsbransjen

Denne saken dreide seg om fiktiv fakturering og bruk av svart arbeidskraft innenfor bygg – og anleggsbransjen, i hovedsak i løpet av 2008 og 2009. Det ble opprettet en rekke firma uten reell drift som utstedte fiktive fakturaer til en oppdragsgiver som gav inntrykk av å ha satt ut jobben på en underleverandør, men som egentlig selv var firmaet som utførte jobben. Dette firmaet hadde uregistrerte lavtlønnede arbeidere med utenlandsk opprinnelse som utførte arbeidet. Etter at firmaene som hadde utstedt de fiktive fakturaene mottok oppgjør inn på sin firmakonto, ble pengene umiddelbart tatt ut i mindre kontantbeløp.

Etter hvert som politiet begynte å avhøre personene som stod som innehavere av firmaene som sendte ut de fiktive fakturaene, forklarte de seg om en bakmann som hadde hjulpet dem med å opprette firmaene, og som fulgte dem rundt når de skulle opprette firmakonto i bank. Så fort de mottok oppgjør for sine fiktive fakturaer, og pengene var tatt ut igjen, samlet bakmannen inn kontantene og fordelte pengene videre tilbake til de som hadde utført den virkelige jobben, og til de som skulle ha en andel i summen for å ha hvitvasket pengene. I løpet av 2009 lyktes det politiet å identifisere den omtalte bakmannen i saken, og han ble pågrepet i Budapest høsten 2009. Innen vedkommende ble utlevert til Norge og man identifiserte telefonnummeret hans, hadde det gått for lang tid til at man kunne sjekke basestasjonsbevegelsene på aktuelt telefonnummer for å sammenholde dette med forklaringene til firmainnehaverne for å bekrefte eller avkrefte det som hadde blitt opplyst i avhør. Med et halvt år eller et års lagringstid ville man kunne innhentet trafikkdata som dekket de fleste gjerningstidspunktene.

2.4.2 Operasjon Lefdal

Høsten 2008 ble det utført en rekke grove bedragerier mot tre ulike fornærmede som fikk tappet sine konti ved at en gjerningsmann møtte opp i banken og gav seg ut for å være kontoinnehaver ved hjelp av falsk legitimasjon. Bedrageriene beløp seg (inkludert forsøk) til ca NOK 3,5 millioner. I samarbeid med sikkerhetsavdelingen i DnB Nor klarte politiet å identifisere gjerningspersonen på et tidlig tidspunkt i saken. Det ble hentet inn trafikkdata fra hans telefon. For noen av bedrageriene viste det seg at gjerningsmannen hadde hatt med seg sin privattelefon, og aktuelle basestasjoner på denne telefonen korresponderte dermed med gjerningssted til rett tid.

Etter at gjerningsmannen ble pågrepet og foreholdt de aktuelle bevis i saken, tilsto han til slutt forholdet.

2.4.3 Operasjon Plastic Fantastic

Denne saken startet med en rekke bedragerier utført av enkeltpersoner i første halvdel av 2007. Man tappet konti til rike personer med falske kort og falske pass ved at gjerningspersonen gav seg ut for å være "den rike".

I juni 2007 begynte politiet å se en sammenheng mellom sakene og koordinere opplysningene. Det viste seg etter hvert at en organisasjon med flere ledd stod bak. Sommeren 2007 var politiet i posisjon til å hente inn trafikkdata på "første bakmannsledd", som hadde fulgt en del av gjerningspersonene rundt i bankene i forbindelse med at kontoene skulle tappes. Flere av disse bakmennene ble pågrepet og fengslet i dette tidsrommet. Samtlige nektet straffeskyld. Etter å ha analysert trafikkdata for disse bakmennene, fant politiet at de hadde telefonkontakt med gjerningspersonene både før og etter at bedrageriene fant sted. Disse funnene er av avgjørende verdi i saken, all den tid bakmennene selv ikke tilstår.

I løpet av høsten 2007 opplevde man imidlertid at bedrageriene fortsatte med samme modus, til tross for at flere sentrale personer var varetektsfengslet. Etter en ny runde med etterforskning i saken, avdekket politiet våren 2008 produksjon av falske pass, en insider ansatt i DnB Nor og en hovedmann. Dette førte til pågripelse av en rekke personer i starten av mars 2008. De straffbare forholdene i saken befant seg derimot innenfor året 2007. Innen man hadde avdekket de mest sentrale personene i denne organisasjonen, og ikke minst insideren i DnBNor, hadde det gått for lang tid til at man kunne hente inn trafikkdata som kunne underbygge dagens siktelse som lyder på organisering grove bedragerier etter §60a i straffeloven, samt grov korrupsjon.

Totalt sett har ca 30 personer vært mistenkt eller siktet i saken, som er berammet til høsten 2010.

3 Bemerkninger til problemstillinger som er fremhevet i høringsnotatet

3.1 Generelle synspunkter

Ovennevnte eksempler viser viktigheten av teledata. Det fremstår som åpenbart at sakene ikke ville blitt oppklart dersom politiet ikke hadde hatt tilgang til trafikkdata. Lengre lagringstid ville også gitt viktig informasjon i saker politiet ikke har lyktes med å oppklare.

Oslo politidistrikt savner en nyansering av hvilke personvern hensyn som med tyngde gjør seg gjeldende. Kontrollert og begrenset lagring av trafikkdata til bruk for offentlige kontrollmyndigheter etter et konkret begrunnet behov, kan vanskelig ses på som problematisk ut i fra generelle personvern betraktninger. Dette gjelder særlig i lys av formålet med lagringsplikten og viktigheten teledata har i bekjempelsen av alvorlig kriminalitet.

Teletilbydere og andre som behandler informasjon av langt mer inngripende karakter, kan etter egen vurdering og forretningsmessig begrunnelse, lagre så lenge de mener det er nødvendig – riktignok under kontroll av Datatilsynet. Når informasjonen skal legges inn i et langt strengere kontrollregime, til bruk for offentlig kontrollmyndighet, bør det være mindre

problematisk ut i fra personvern hensyn. Oslo politidistrikt har vanskelig for å se hvilke konkrete personvern hensyn som vesentlig bryter ned lagringsplikts omfang og tid.

Oslo politidistrikt vil fremheve at etterforskningen består i informasjonsinnhenting for å opplyse saken så godt som mulig. Etterforskningen er objektiv, og skal også få frem opplysninger som taler for siktedes uskyld. Erfaringsvis er teledata et typisk eksempel som siktede i sakene anfører at politiet må undersøke.

Videre skal det fremheves at enkelte sakstyper er særlig utsatt i forhold til lagringstid, idet anmeldelsen innkommer, eller det straffbare forhold først blir avdekket, etter at teledata er slettet. Problemet forsterkes ytterligere når man ser at teledata er av avgjørende betydning for disse sakstypene. Det kan her kort vises til menneskehandel, hvor feks prostituerte ofte har lagret kunder og bakmenn under kallenavn på sin mobiltelefon, og teledata er det eneste som kan underbygge de prostituerte (den fornærmede) sin forklaring.

Det understrekes også at alvorlig kriminalitet gjennomgående tar tid å etterforske på grunn av sakenes kompleksitet og omfang. Gjennomsnittlig saksbehandlingstid på samtlige avsnitt ligger langt over dagens lagringstid. Politi og påtalemyndighet får svært sjelden kritikk av domstolene for saksbehandlingstid i disse sakene, idet tidsaspektet er begrunnet i arbeidsoppgaver, og anerkjennes av de som får innsyn i sakene.

Vi vil også bemerke at kortere lagringstid og tap av trafikkdata medfører økt bevismessig behov for andre og presumptivt mer inngripende metoder ut fra personvern hensyn. Vi kan eksempelvis nevne det som i høringsnotatet er betegnet som sanntids kommunikasjonskontroll. Dette vil medføre en stor, og unødvendig, arbeidsbelastning for politiet, påtalemyndigheten og retten, og det vil også være mer inngripende for de impliserte i straffesakene. Oslo politidistrikt er derfor av den klare oppfatning at en lovpålagt lagringstid på to år vil være et vesentlig, og nødvendig, bidrag til bekjempelsen av alvorlig kriminalitet.

Avslutningsvis understrekes at teledata har blitt et svært viktig bevis i svært mange av sakene som etterforskes ved Oslo politidistrikt. Teledata gir bl.a. en unik mulighet til å etterprøve sannhetsgehalten i politiforklaringer, tidfeste gjerningstidspunkt og bekrefte hvor de impliserte har oppholdt seg.

3.2 Hvilke typer data bør lagres?

Ut i fra lagringsplikts formål, må det klare utgangspunkt være lagring av alle data som kan tenkes å ha bevismessig betydning i straffesaker.

3.3 Lagringstid og forslaget om ikke å skille lagringstid etter teknologi

Hensynet bak reglene er bekjempelse av alvorlig kriminalitet. Etterforskningen i slike saker er komplisert, omfattende og tidkrevende, hvor bakmenn/gjerningspersoner først blir identifisert og mistenkt etter måneder og år med intensiv etterforskning. Eksempelene fra konkrete saker ved Oslo politidistrikt, viser at teledata er tapt før politiet er i posisjon til å begjære disse utlevert.

En utleveringsbegjæring i en sak ved spesialavsnittene, vil naturlig gå på utlevering av trafikkdata så langt tilbake i tid som selskapet har lagret data. Sakstypene kjennetegnes ved at kriminaliteten utøves over tid og er godt organisert. For enkelte sakstyper vil teledata være slettet, før politiet mottar anmeldelse eller på annen måte avdekker det straffbare

forholdet. Politiet har kjennskap til lagringsrutinene og vil naturlig ikke be om data som en på forhånd vet ikke er lagret. Erfaringer fra de ulike selskapene vedr anmodninger fra politiet kan følgelig ikke tillegges vekt.

Dersom reglene skal tjene formålet, må lagringstiden i direktivet utnyttes fullt ut. Lagringen vil skje på betryggende måte, og vil kun gis ut etter beslutning fra kompetent myndighet. En kan følgelig ikke se at en noe lengre lagringstid vil utgjøre en stor forskjell ut i fra personvern hensyn, og det oppveies av den store betydning lengre lagringstid har for oppklaring av alvorlig kriminalitet.

3.4 Oppregningen av lovbrudd som alternativer til strafferammekravet

Det er foreslått at en istedenfor et generelt krav om at handlingen skal kunne medføre fengsel i tre år eller mer, skal det angis en oppregning av aktuelle straffebud. Oslo politidistrikt er av den klare oppfatning at hensynet til personvern er tilstrekkelig ivarettatt slik grunnvilkåret er i dag. Det skal også bemerkes at det ikke er satt slike vilkår ved vitneforklaring til retten, jf strprl. § 116. Politiet kan altså få samme informasjon fra en ansatt hos teleleverandøren, som evt må medta dokumentasjon til støtte for hukommelsen) uten at det er krav om tre års strafferamme. Det bør derfor ikke stilles for strenge krav til utlevering av teledata. Oslo politidistrikt viser for øvrig til høringsuttalelse som blir gitt til NOU 2009:15 (Skjult informasjon – åpen kontroll). En legger til grunn at lagringsplikten må samkjøres med de endringer som foreslås i NOU 2009:15. Oslo politidistrikt har klare innvendinger til forslagene som er fremmet.

Dagens praksis tilfredsstiller direktivets forutsetning om at det ikke skal gjelde i alle saker. Det blir også i dag foretatt en konkret vurdering i den enkelte sak, slik at det kun innhentes i saker hvor det er et særlig behov. Den enkelte sak hvor teledata begjæres utlevert må således, ut i fra behovet og den konkrete vurderingen, også karakteriseres som ”særlig”.

Ved etterforskning av alvorlig kriminalitet, vil det i visse tilfeller være nødvendig å etterforske andre mindre alvorlige straffbare forhold opp i mot et miljø eller person for å bygge opp en sak. I en slik informasjonsinnhentingsfase vil trafikkdata være en viktig kilde. Informasjonen vil erfaringsvis gi skjellig grunn til mistanke opp i mot den kriminalitet som politiet mistenker miljøet for å bedrive. Til dette kommer at nettopp innhenting av teledata under etterforskningen av en ordinær straffesak, fører til at man avdekker at kriminaliteten er grov.

En vil også miste muligheten til å innhente trafikkdata i saker som vi i dag ikke kan tenke oss som ”særlige”, men som kan vesentlig endre karakter. Det kan også tenkes kriminalitetstyper som vi i dag ikke er plaget av, men som kan oppstå i stor omfang.

3.5 Forslag om at kun retten skal kunne pålegge besitteren å utlevere data

Kompetansen til å begjære teledata utlevert bør ligge hos påtalemyndigheten, som er den nærmeste til å vurdere viktigheten av teledata i den enkelte sak. Datalagringsdirektivet stiller ingen krav til nasjonal lovgivning på dette punktet, og en kan ikke se behovet for en begrensning av påtalemyndighetens kompetanse. Oslo politidistrikt kan ikke se at dette er nærmere begrunnet. En generell henvisning til at omfanget av innhenting av trafikkdata er stort, kan ikke tas til inntekt for at myndigheten bør legges til domstolene. Dette tilsier kun at betydningen av trafikkdata i etterforskningen er stor.

Erfaringene tilsier at rettsikkerheten er ivaretatt med dagens ordning, og en overføring av ansvaret til retten vil følgelig ikke være et begrunnet bidrag til økt rettsikkerhet. Samtlige som arbeider i påtalemyndigheten har juridikum, og de personene som arbeider med organisert kriminalitet har gjennomgående også lang arbeidserfaring. Påtalemyndigheten har ansvaret for etterforskningen og at straffeprosessen blir fulgt, og en mener det kan legges til grunn at ansvaret blir gjennomført på en betryggende måte.

En overføring av myndigheten til retten, vil bidra til en vesentlig økt saksbehandling og ressursbruk hos politiet, påtalemyndigheten og tingretten. I hver enkelt sak må tingretten få oversendt påtegning med begrunnelse for begjæringen og kopi av samtlige saksdokumenter – pr. i dag er dette omlag 1900 saker årlig. Dette vil være en unødvendig tapping av politiets og tingrettens ressurser, uten at det vil være et begrunnet bidrag til økt rettsikkerhet.

Oslo politidistrikt viser for øvrig til høringsuttalelse som blir gitt til NOU 2009:15 (Skjult informasjon – åpen kontroll).

3.6 Utformingen av vilkåret for skjellig grunn til mistanke

Et krav om at ”noen med skjellig grunn mistenkes”, vil frata politiet muligheten til å innhente avgjørende bevis/trafikkdata i svært mange saker. I et stort antall saker som etterforskes ved spesialavsnittene - alvorlig kriminalitet - foreligger det skjellig grunn til mistanke om en straffbar handling, men ikke til en bestemt person. Vi nøyer oss her med å vise til drap, overfallsvoldtekter og annen grov moduskriminalitet begått over tid, hvor teledata vil være svært viktig for å lokalisere tidspunkt for vitner/impliserte, hvem som har vært i det aktuelle området osv.

En slik skjerpning av grunnvilkåret vil medføre en klar begrensning i politiets mulighet til å oppklare alvorlig kriminalitet, hvilket klart strider mot selve formålet med lagringsplikten.

Oslo politidistrikt mener at rettsikkerheten er ivaretatt slik reglene er utformet i dag. Vi viser også til høringsuttalelse som blir gitt til NOU 2009:15 (Skjult informasjon – åpen kontroll).

4. Generelle synspunkter fra avdelingene

4.1 Synspunkter fra etterforskning og påtale ved seksjon Organisert Kriminalitet

Teledata er svært viktig i samtlige av sakstypene som behandles ved avdeling for organisert kriminalitet, enten det gjelder grov narkotikakriminalitet, menneskehandel eller gjeng/bande. Etterforskningen retter seg ofte mot bakmenn i Norge og utlandet, som benytter et omfattende nettverk som stråmenn. Kommunikasjon står sentralt også i de kriminelle nettverkene, og elektroniske spor er svært ofte avgjørende for å vise knytningene i miljøet og bevegelser/lokalisering på gjerningstidspunktet. Slik etterforskning, spesielt over landegrensene, er svært tidkrevende, og teleleverandørenes lagringstid er ofte overskredet når etterforskningen løpende avdekker sentrale aktører.

4.2 Generelle synspunkter fra Analyse ved seksjon for Organisert Kriminalitet

Innhenting av trafikkdata på ulike telefonnummer er av vesentlig betydning for oppstart av en sak med kommunikasjonskontroll, men også for den videre etterforskningen. Trafikkdata er av vesentlig betydning da det gir oss informasjon omkring

- kontaktnett/omgangskrets: (A og B nummer): viser kontaktnettet /omgangskretsen til den som disponerer telefonnummeret. Viser utenlandskontakter, gir et inntrykk av hvilke personer som har nær tilknytning til disponent av telefonnummeret, interessante utenlandske kontakter kan avdekkes, og andre interessante personer i disponentens nettverk eller som er kjent for politiet for øvrig.
- dato/tid(klokkeslett): gir oss et inntrykk av hva slags telefonkontakt disponenten av nummeret har til hvilken tid på døgnet, samt at man kan se hvor disponenten(telefonnummeret)befinner seg når telefonkontakten finner sted
- oppholdssteder: (basestasjoner) kan være bopel, arbeidssted, utenlandsopphold, interessante andre geografiske tilknytninger
- Imei: Vi kan se om disponenten bruker telefonnummeret i flere telefonapparater

Det er av vesentlig betydning for både skjult/åpen etterforskning at vi mottar informasjonen i trafikkdata så langt tilbake i tid som mulig. Det viser seg ved flere tilfeller at man i etterforskningsprosessen får kjennskap om viktige telefonnummer/imeinummer som har vært brukt av personer som har en sentral rolle i saken etter noe tid. Ved forsøk på innhenting av informasjon på disse viser det seg at mye informasjon ofte er slettet/gått tapt da det overstiger lagringstiden til teleselskapene.

4.3 Generelle synspunkter fra seksjon Vold og sedelighet

Et tenkt eksempel hvor lengre lagringstid vil være et vesentlig bidrag til sakens opplysning og tiltaltes forsvar, er nye opplysninger som kommer opp i løpet av etterforskningen og under rettssaken. Etterforsker og aktor har i flere tilfeller mottatt henvendelser fra forsvarer, eller ny forsvarer, som i ettertid ønsker at politiet skal innhente trafikkdata fra et annet tidsrom enn det som har blitt sikret underveis i etterforskningen. Materialet vil da gjennomgående være slettet. En viser for øvrig til eksempel under punkt 2.3.10.

Politiet er avhengig av å verifisere opplysninger generelt, også de som er fremsatt av en i utgangspunktet ”fornærmet”. I våre saker kan ofte teledata være eneste mulighet til å bekrefte/avkrefte fremsatte påstander i avhør. Det er flere eksempler fra Sedelighetsavsnittet hvor opplysningene brukes til å snu sakene – d.v.s. til å vise at opplysningene og anklagene som kommer fra ”fornærmede” som anmelder forholdet, ikke kan stemme. På denne måten forhindrer vi at uskyldige blir dratt igjennom et langvarig politi- og rettsapparat og kanskje til slutt uskyldig dømt. Dette er viktig for rettssikkerheten!

Det er et generelt behov i overfallssaker/voldtektssaker med ukjent gjerningsmann, eller moduskandidater i serievoldtektssaker hvor det ikke forefinnes annet i saken enn fornærmedes forklaring og anmeldelse i tillegg til likhetstrekk og samme modus ved flere gjentakende forhold over tid/flere år. Ved å ha tilgang til basesøk og lagret trafikkdata lenger tilbake i tid enn det som nå er mulig, kunne politiet avdekket om vedkommende befant seg i gitt område på tid og sted for anmeldt forhold. Dermed vil politiet ha et bedre og annet grunnlag for å etterforske videre – enten for å kunne sannsynliggjøre at vedkommende faktisk var i det aktuelle området, eller på den annen side for å kunne fjerne mistanken mot vedkommende i den enkelte sak.

Dette vil ikke alene gi et godt nok svar, men det gir en indikasjon og noe å jobbe videre med – evt. sammenholdt mot øvrige opplysninger i den enkelte sak.

4.4 Generelle synspunkter fra seksjon for Finans og miljø

Trafikkdata har nå en sentral plass i en rekke av sakene som etterforskes på avsnittet. Erfaringsmessig er vi en avdeling som ikke mottar aktuelle saker (med unntak av brannsaker) før det har gått en god stund. Det er flere årsaker til dette, men en viktig årsak ligger i at økonomisk kriminalitet kan være vanskelig å oppdage, og det er ikke sjelden at det straffbare forhold kan ligge et halvt til ett år tilbake i tid på det tidspunktet vi mottar anmeldelse.

Dette har ført til at vi i flere konkrete tilfeller hvor trafikkdata hadde vært aktuelt ikke har hatt mulighet til å vurdere dette, da det straffbare forholdet har skjedd for langt tilbake i tid. Dette har avskåret oss både fra å innhente avgjørende bevis for å pådømme eventuelle gjerningspersoner samt tilsvarende å sjekke aktuelle personer ut av saken.

Med vennlig hilsen

Anstein Gjengedal

Saksbehandler:
Per Håkon Sand, Hege
Naustdal mfl./RB