POLITIET

Samferdselsdepartementet

Postboks 8010 Dep
0030 Oslo

Deres referanse	*Vår referanse*	*Dato*
09/585-HK	201000096/4	12.04.10

DATALAGRINGSDIREKTIVET - HØRINGSSVAR FRA KRIPOS

Innledning

Innføring av Datalagringsdirektivet vil sikre at trafikkdata er tilgjengelig for politiet i forbindelse med etterforskning av alvorlig kriminalitet. Lagring av denne type data er ikke noe nytt, men trafikkdata er i ferd med å bli mindre viktig for teletilbydernes interne formål, hvilket indirekte reduserer politiets tilgang til denne typen bevis. Derfor mener Kripos det er viktig å sikre at forutsetningene for fortsatt oppklaring av alvorlige forbrytelser formaliseres. Datalagringsdirektivet er i den forbindelse et egnet instrument.

Kripos anbefaler sterkt at Datalagringsdirektivet innføres, men at det gjøres endringer i forslagene til den nasjonale implementeringen av direktivet i Norge. Begrunnelsen for dette følger av den nærmere redegjørelsen i *del V – del VII*.

Innledningsvis vil vi i *del I* kort kommentere Datalagringsdirektivets formål og gi en kort beskrivelse av den teknologiske utviklingen.

Innføringen av Datalagringsdirektivet stiller ulike hensyn opp mot hverandre; samfunnets behov for å oppklare og iretteføre forbrytelser, borgernes rett til personvern og forhold knyttet til teletilbydernes konkurransevilkår.

Kripos vil i denne sammenheng påpeke at den manglende kartlegging av politi og påtalemyndighets behov for denne type bevis, fremstår som en åpenbar svakhet ved høringen. I høringsuttalelser som allerede er offentliggjort fremgår det tydelig at høringsinstanser savner informasjon om dette, og også til dels misforstår viktige sider av dette tema. Dette innebærer igjen at de ikke har muligheter for å foreta en balansert avveiing av de kryssende hensyn som gjør seg gjeldende. Det samme gjelder i forhold til de konsekvenser som de foreslåtte endringer i den internrettslige regulering vil innebære i forhold til dagens gjeldende regelverk. Etter vårt syn er det uheldig at disse spørsmål ikke var utredet forut for høringen og det er grunn til å anta at dette kan ha direkte betydning for enkelte instanser konklusjoner.

Kripos
Den nasjonale enhet for bekjempelse av organisert og annen alvorlig kriminalitet
Brynsalléen 6, Postboks 8163 Dep, 0034 OSLO
Tlf.: (+47) 23 20 80 00 Faks: (+47) 23 20 88 80
E-post: kripos@politiet.no Org.nr.: 974 760 827

Kripos har av denne grunn valgt å vie politiets behov for trafikkdata betydelig oppmerksomhet i høringssvaret. I *del II* av høringssvaret har vi har å gi en utfyllende beskrivelse av politiets behov knyttet til ulike sakstyper, samt at vi i *del III* beskriver omfanget og nytteverdien av trafikkdata. Her beskrives også en undersøkelse Kripos nylig har gjennomført vedrørende nytteverdi av trafikkdata i saker fra 2008.

I *del IV* har vi kommentert noen generelle spørsmål i tilknytning til høringsnotatet, før vi i *del V* behandler spørsmålene om lagringstid, sikringspålegg og politiets tilgang til trafikkdata.

I *del VI* kommenterer vi de foreslåtte endringene i straffebudene i straffeprosessloven og ekomloven.

Videre behandler vi spørsmålene om hvilke data som bør lagres og valg av lagringsløsning i *del VII*.

Endelig oppsummerer vi kort hovedtrekkene i høringssvaret i *del VIII*.

DEL I – Kort om datalagringsdirektivets formål og den teknologiske utvilklingen

1.1 Datalagringsdirektivets formål

Trafikkdata lagres i dag på bakgrunn av teletilbydernes fakturerings- og driftssikkerhetsbehov, og ikke av hensyn til kriminalitetsbekjempelsen. På samme måte som politiet innhenter informasjon fra eksempelvis bompengepasseringer, videoovervåkingskamera, fordelskort hos flyselskaper, hotellister mv. kan også trafikkdata innhentes i forbindelse med etterforskning, såfremt slike data er tilgjengelige når behovet oppstår.

Myndighetene kan hensyn til kriminalitetsbekjempelsen velge å innføre en plikt til å ta vare på visse typer informasjon som erfaringsmessig har stor betydning for oppklaringen av straffesaker. En slik plikt foreligger allerede for registrering av valutatransaksjoner. Etter hvitvaskingsloven plikter alle rapporteringspliktige å registrere både navn, fødselsnummer og adresse på alle som utfører valutatransaksjoner som gjelder kr 100 000,- eller mer, uavhengig av om det foreligger mistanke om en straffbar handling. Lovgiver har i dette tilfellet gjort en avveiing, og funnet at hensynet til kriminalitetsbekjempelsen rettferdiggjør inngrepet. Dokumentasjon skal oppbevares i fem år etter transaksjonen ble utført eller kundeforholdet ble avsluttet. Grunnen til dette er at det er potensielt bevismateriale i en straffesak. Formålsparagrafen, §1, lyder slik: *"Lovens formål er å forebygge og avdekke transaksjoner med tilknytning til utbytte av straffbare handlinger eller med tilknytning til terrorhandlinger."*

Siden teletilbyderne per i dag ikke har noen plikt til å lagre trafikkdata vil det være mer eller mindre tilfeldig hvorvidt de nødvendige dataene eksisterer når politiet har behov for å innhente dem.

Det er på det rene at teletilbydernes behov for å lagre trafikkdata for faktureringsformål i løpet av få år vil være borte. Årsaken til dette er at teletilbyderne i stor grad går over til abonnementstyper med fastpris. Fakturering med bakgrunn i abonnentens bruk er derfor

ikke lenger relevant. Dermed forsvinner også muligheten til å innhente og bruke trafikkdata som bevis i straffesaker, til tross for at hjemmelen er til stede. Dataene vil i stor utstrekning fortsatt bli generert av hensyn til teletilbyderens driftssikkerhet, men dataene vil bli slettet etter kort tid.

Innføringen av Datalagringsdirektivet i EU er en erkjennelse fra de europeiske landene av at trafikkdata har blitt et så viktig spor i etterforskning av alvorlig kriminalitet at lovgivningen må sikre at sporene vil være tilgjengelige også for fremtiden. Særlig viktig er dette siden teletilbydernes behov for denne typen opplysninger blir mindre i fremtiden.

Innføring av direktivet gir en forutsigbarhet for hvilke potensielle bevis som vil være tilgjengelige. Derfor er direktivet viktig for politiets evne til å oppklare og forebygge forbrytelser, samt utføre politioppgaver i forbindelse med saknetsaker, redningsaksjoner og ulykker.

En av innvendingene til direktivet, som ofte fremsettes, er at lagringen representerer et inngrep overfor alle borgere, og ikke bare de som mistenkes for straffbare handlinger. Dette er ikke unikt, og kan eksempelvis sammenlignes med myndighetenes grensekontrollvirksomhet, som retter seg mot enhver som passerer grensen. Dette representerer et inngrep overfor uskyldige, men rettferdiggjøres av formålet med kontrollen. Det er ikke tvilsomt at grensekontrollen som utføres jevnlig bidrar til å avdekke kriminalitet. På samme måte må en vurdere om lagring av trafikkdata rettferdiggjøres av formålet med lagringen. I den forbindelse vil betydningen av historiske trafikkdata i etterforskningen være et vektig moment, jfr del II nedenfor. Virkemiddelet må være formålstjenlig for å rettferdiggjøre inngrepet det medfører.

1.2 Teknologisk utvikling

Fra NOU 2007:2 "Lovtiltak mot datakriminalitet"[1] siteres følgende:

> *Lovgivningens oppgave er å regulere virkeligheten. For å regulere datakriminalitet må lovgiver ta utgangspunkt i den faktiske situasjonen i samfunnet, og her har det oppstått store endringer på grunn av utviklingen av datateknologien. En kan snakke om en revolusjon som er av like stor betydning som den industrielle revolusjon var i sin tid. Datateknologien har skapt nye muligheter, men også farer og trusler. Informasjons- og kommunikasjonsteknologien (IKT) er i dag blant samfunnets viktigste infrastrukturer. Oppstår det alvorlige problemer på denne sektoren, kan også vitale samfunnsinteresser bli skadelidende. Det er derfor viktig med en strafflovgivning som gjenspeiler dagens trusler.*
>
> *Internett har gitt nesten ubegrensede muligheter til kommunikasjon og informasjonsformidling. Dette har igjen åpnet for en utvikling i samfunnet som for noen tiår siden var utenkelig. Enorme mengder informasjon kan publiseres ett sted i verden, for å være tilgjengelig et helt annet sted i løpet av sekunder. Internett brukes daglig av folk over hele verden. Det foreligger betydelige utfordringer tilknyttet straffeforfølgning på tvers av landegrenser for forbrytelser foretatt ved bruk av internett. Det er ofte vanskelig å identifisere forbryterne, og dersom man klarer det, vil de ofte forsvare seg med at handlingene er utført i et annet land der serveren stod, eller at de befinner seg i et land hvor de ikke kan forfølges eller som ikke vil utlevere vedkommende til et annet land. Gjennom nettets relativt korte historie har det likevel vist seg at kontroll av internett og forfølgning av lovbrytere på nettet er mulig.*

[1] NOU 2007:2 Lovtiltak mot datakriminalitet, kapittel 3 Det faktiske landskapet, pkt 3.1. Innledning

Som følge av den virkelighet som beskrives av Datakrimutvalget står politiet overfor nye utfordringer. Allerede i dag er en vesentlig del av politioppgavene på internett. Fremtidens politimetoder må derfor ta høyde for dette. Den nye straffeloven av 2005, som foreløpig ikke har trådt i kraft, har på flere områder tatt høyde for den utvikling som er beskrevet ovenfor. Kapittel 21 inneholder bestemmelser om vern av informasjon og informasjonsutveksling. I tillegg til å ha de nødvendige straffehjemler, er det også nødvendig at de prosessuelle hjemler – politimetodene – tar høyde for utviklingen.

Når politiet beveger seg i den virtuelle verden må en ha samme mulighet til å sikre bevis der som i den virkelige verden. Det er heller ikke snakk om et enten-eller. Det vil som regel være nødvendig å innhente både elektroniske og fysiske bevis for å oppklare en straffesak. Hvis ikke begge deler er tilgjengelig vil bevisbildet ikke bli fullstendig.

Den teknologiske utviklingen har medført at stadig mer kommunikasjon blir IP-basert ved at internett benyttes som databærer. Husstander og bedrifter går over til IP-basert telefoni, mobiltelefoner har mulighet for å ringe via trådløse nettverk ved bruk av eksempelvis Skype og datamaskiner brukes i stor grad til kommunikasjon, blant annet gjennom mail, chat, nettsamfunn, fildeling mv. For å kunne identifisere avsender/mottaker er en avhengig av å kunne knytte de aktuelle IP-adressene til et bestemt sted eller en bestemt person. Dette har gjort at politiets behov for lagring av abonnementsdata for IP-adresser har økt vesentlig de siste årene. Dette gjelder for en rekke sakstyper. Særlig godt kommer det til syne ved etterforskning av internettrelaterte seksuelle overgrep og spredning av overgrepsmateriale mot barn, hvor internett som kommunikasjonsmedium er helt sentralt[2].

Denne utviklingen understreker viktigheten av å ha et teknologinøytralt regelverk[3] for lagring av trafikkdata slik direktivet legger opp til, hvor politiets muligheter for å finne spor er uavhengig av om kommunikasjonen har foregått via internett eller via telefon. Ellers vil de kriminelle søke til kommunikasjonsformer de vet at politiet ikke kan spore. Per i dag er det stor forskjell på politiets mulighet til å spore kommunikasjon på internett, eksempelvis via sosiale medier, og muligheten til å spore telefontrafikk. Det er et faktum at enkelte kriminelle tilpasser seg dette.

En kan derfor stille spørsmål om innføringen av direktivet vil medføre at de kriminelle finner måter å omgå det på. Kripos er godt kjent med problemstillingen, og mener at den ikke på noen måte er et argument mot å innføre direktivet. Når fingeravtrykksundersøkelser fikk sitt gjennombrudd på starten av 1900-tallet ble det hevdet at alle kriminelle ville bruke hansker. Fingeravtrykksundersøkelser oppklarer fortsatt et stort antall saker hvert år. Enkelte hevdet også at kommunikasjonskontroll av mobiltelefoner ville ha mindre effekt når andre kommunikasjonsmedium som epost, sosiale medier og kommunikasjonstjenester som Skype ble innført. Avlytting av telefoner er fortsatt et viktig verktøy for politiet, og dette fremkommer også i Metodekontrollutvalgets[4] ferske evaluering av politiets metoder. Samtidig viser det seg at politiet har stor nytte av trafikkdata til tross for at de kriminelle er godt kjent med at dette er spor politiet undersøker.

---

[2] Se også beskrivelse av den teknologiske utviklingen i NOU 2009:15, pkt 8.6.2, s 78, 2.spalte

[3] Mht teknologinøytralt regelverk: i Rt. 1999/1944 slo Høyesterett fast at politiet kunne få tilgang til abonnentopplysninger for internett, ved å sammenligne dette med at politiet allerede hadde potensiell tilgang til abonnentopplysninger for telefonnummer som ikke sto i katalogen. Med andre ord så Høyesterett behovet for å bruke like regler på ulike teknologier.

[4] NOU 2009:15 – kapittel 10, s 114 flg

De kriminelle vil alltid ta hensyn til politiets kapasitet og metodebruk. Dette betyr derimot ikke at saker ikke er mulige å oppklare. Nokas-saken er et godt eksempel på dette. Til tross for grundige forberedelser og foranstaltninger mot politiets etterforskning ble saken likevel oppklart, og bruk av trafikkdata og andre elektroniske spor hadde avgjørende betydning i etterforskningen. Derimot gjør de kriminelles motstrategier sakene mer kompliserte og tidkrevende å etterforske, blant annet å finne frem til hvilke telefoner de mistenkte har benyttet. Denne profesjonaliteten er et vektig argument for lagringstidstidens lengde. Dette kommer vi tilbake til under pkt 5.1.

For øvrig er det et faktum at en stor del av den alvorlige kriminaliteten, herunder draps- og voldtektshandlinger, er impulshandlinger hvor gjerningspersonen ikke har tatt spesielle forhåndsregler i forkant.

DEL II – Politiets behov for trafikkdata for å etterforske alvorlig kriminalitet

Kripos vil i det følgende - gjennom sakseksempler som har vært omtalt i media - gi en beskrivelse av behovet for trafikkdata. Politiets behov for innhenting av trafikkdata må ses i naturlig sammenheng med domstolenes behov for å få denne informasjonen framlagt for å kunne belyse saken tilstrekkelig til å avsi dom, jfr strpl §294.

Trafikkdata er en type bevis som normalt veier tungt i bevisvurderingen, fordi de er objektivt konstaterbare. I en sak hvor store deler av handlingen har utspilt seg i cyberspace vil det bli nærmest umulig å avsi dom dersom retten mister muligheten til å benytte disse objektive holdepunktene i sin bevisvurdering.

Kripos baserer den videre gjennomgangen i all hovedsak på saksområder som ligger innenfor Kripos' ansvarsområde, jfr påtaleinstruksen kap 37, og saker hvor Kripos normalt gir bistand til politidistriktene. Det understrekes at andre politi- og påtalemyndigheter kan ha andre erfaringer og behov, særlig gjelder dette de øvrige særorganene.

2.1 Beskrivelse av politiets bruk av trafikkdata i etterforskningen

Politiet har siden midten av 90-tallet brukt trafikkdata regelmessig i etterforskning av alvorlige straffesaker. Bruken av denne typen spor økte i takt med økningen i bruken av mobiltelefon i samfunnet.

Etter hvert har trafikkdata blitt viktig for en rekke sakstyper. Sporene kan deles inn i to hovedgrupper; personspesifikke og stedsspesifikke spor. De personspesifikke sporene er utskrifter som knyttes til en bestemt person eller til et bestemt telefonnummer/dataanlegg, mens de stedsspesifikke sporene er spor som knytter seg til et bestemt geografisk område, eksempelvis en oversikt over all telefontrafikk i nærheten av et drapsåsted. Begge sportypene er av stor betydning for etterforskningen.

De personspesifikke sporene er i hovedsak utskrifter som viser historisk trafikk for et bestemt telefonnummer eller hvem som har benyttet et bestemt dataanlegg (IP-adresse - abonnementsdata). Telefonutskriftene gir i hovedsak to typer opplysninger; hvem mistenktes/fornærmedes/vitnets telefon har vært i kontakt med og hvor telefonen har befunnet seg når samtaler er foretatt (basestasjon).

Denne typen opplysninger er av stor betydning blant annet for å kontrollere forklaringer og for å avdekke ytterligere impliserte i saken. Utfordringen med personspesifikke spor er å avdekke hvilke telefonnummer / IP-adresser som er relevante før dataene går tapt. De mistenkte er klar over at politiet bruker denne typen spor, og forsøker å vanskeliggjøre politiets etterforskning ved hyppig bytte av telefonnummer, benytte telefonnummer registrert på andre personer (ofte fiktive personer) og ved at det brukes bestemte nummer kun for én straffbar handling. Andre personspesifikke spor som brukes i etterforskning (som ikke er trafikkdata) er eksempelvis utskrift av mistenktes bankkonto, utskrift av bompengepasseringer fra mistenktes bil, bruk av betalingskort/nøkkelkort osv.

De stedsspesifikke sporene er for trafikkdata i hovedsak såkalte basestasjonsutskrifter. Dette gir oversikt over alle samtaler foretatt i et bestemt geografisk område. Utskriftene innhentes for en kortere tidsperiode, eksempelvis alle samtaler i nærheten av åstedet for i tiden like før/etter et antatt drapstidspunkt. Gjennom disse utskriftene vil man få oversikt over personer som har befunnet seg i nærheten av åstedet på gjerningstidspunktet. I tillegg til at opplysningene kan gi informasjon om mulig gjerningsmann vil de også kartlegge viktige vitner. Andre stedsspesifikke spor som benyttes i etterforskningen (som ikke er trafikkdata) er eksempelvis utskrifter fra alle passeringer i bomringen, video fra overvåkingskamera, utskrift av transaksjoner fra en bestemt minibank osv.

Forslaget i høringsnotatet[5] er at det skal innføres et krav om at "*noen med skjellig grunn mistenkes*". Dette vil medføre at muligheten til å benytte trafikkdata i identifiseringsøyemed - ved å sikre stedsspesifikke data - bortfaller. Vi kommer tilbake til dette i pkt 5.3.2.2.

2.2 Forholdet til andre metoder

Politiet har en rekke ulike metoder for å etterforske alvorlig kriminalitet. De ulike metodene utfyller hverandre og har ulik nytteverdi. Som oftest er ikke én metode alene avgjørende; det er samspillet mellom flere relevante metoder som oppklarer saken. Politiets bruk av trafikkdata i etterforskningen kan ikke erstattes av andre eksisterende metoder.

Departementene har også vurdert dette i høringsnotatet og kommet til at det ikke finnes noe alternativ til trafikkdata[6]. Kripos støtter dette synet.

Trafikkdata vil kunne bidra til å rekonstruere et hendelsesforløp gjennom å se på de mistenktes bevegelser eller kontaktmønster. Politiets ulike metoder beskrives gjerne som "politiets verktøykasse". I denne "verktøykassen" er trafikkdata ett av de helt avgjørende basisverktøyene. Det er et verktøy som hver eneste dag bidrar vesentlig til oppklaring av alvorlige forbrytelser. Ingen andre metoder gir den samme type informasjon og det finnes ikke noe alternativ til trafikkdata i "politiets verktøykasse".

Trafikkdata har feilaktig blitt sammenlignet med kommunikasjonskontroll. Selv om begge metodene dreier som om kontroll av kommunikasjon er det to vesentlige forskjeller. Trafikkdata gir ingen informasjon om kommunikasjonens innhold. Og kommunikasjonskontroll gir ingen historisk informasjon; en vil kun få informasjon om samtaler som finner sted etter at kommunikasjonskontrollen er iverksatt.

Politiet har de senere årene fått nye metoder, blant annet romavlytting og muligheter for å unnlate varsling av mistenkte ved ransaking, beslag og utleveringspålegg. De nye metodene

[5] Høringsnotatet, pkt 4.12, s 48
[6] Høringsnotatet, pkt 4.2, s 28, 3.avsnitt

er i hovedsak anvendelige ved proaktiv etterforskning. Man kan selvsagt også bruke disse skjulte metodene i eksempelvis en drapssak, og håpe at mistenkte røper informasjon i samtaler med andre, eller at en ved ransaking med utsatt underretning ("hemmelig ransaking") vil finne viktige bevis. Men det er viktig å understreke at ingen av disse metodene kan *erstatte* trafikkdata; de kan bare supplere. De nye metodene er med på å gi politiet et (nødvendig) større spekter av etterforskningsmetoder.

2.3 Beskrivelse av aktuelle sakstyper og eksempler fra saker

Nedenfor vil vi beskrive politiets behov for trafikkdata ved å redegjøre for hvordan person- og stedsspesifikke spor har blitt brukt og brukes i politiets etterforskning. Med konkrete henvisninger til saker innenfor sakstypene *drap*, *saknet person*, *narkotika*, *grove ran*, *seksuelle overgrep*, *internettrelaterte seksuelle overgrep*, *vinning* og *datakriminalitet*. Sistnevnte sakstype skiller seg helt fra de øvrige sakstypene ved at den kriminelle handlingen foregår på det elektroniske mediet selv ("subject of the crime"). De øvrige sakstypene benytter det elektroniske mediet til gjennomføringen av eller planleggelsen av den kriminelle handlingen ("assistance in the crime").

Det er utfordrende å gi en generell beskrivelse av alle formål trafikkdata fyller i etterforskningen siden ingen etterforskning er lik, men vi vil nedenfor beskrive enkelte sakstyper hvor trafikkdata er et sentralt bevismiddel, og gi noen forenklede eksempler fra saker. Beskrivelsen innbefatter de sakstyper Post- og teletilsynet[7] har oppgitt som de hvor politiet hyppigst anmoder om fritak fra taushetsplikten etter ekomloven.

Samtidig er det slik at det ikke nødvendigvis fremkommer i domsgrunnene hvorvidt trafikkdata har vært viktig for oppklaringen av saken. Domstolens behandling gir et bilde av resultatet av etterforskningen, og bare i liten grad hvordan etterforskningen forløp. Trafikkdata kan ha vært av stor betydning for etterforskningen selv om det ikke fremkommer under hovedforhandlingen. Trafikkdata benyttes ofte innledningsvis, for å identifisere mistenkte og gi grunnlag for annen bevissikring, som innhenting av DNA-prøve, ransaking og avhør. Betydningen av trafikkdataene vil i slike tilfeller sjelden være omstridt, og dermed heller ikke gjenstand for bevisvurdering i retten. Det at trafikkdata forefinnes vil også gi en prosessøkonomisk effekt, idet tiltalte sjelden vil benekte omstendigheter som er ugjendrivelig bevist.

2.3.1 Drapssaker

Undersøkelser foretatt av Kripos viser at trafikkdata innhentes i ca 75% av alle drapssaker[8]. Utfordringene med etterforskningen av drapssaker kan være vidt forskjellig, - fra en sak hvor gjerningsmannen blir tatt på fersk gjerning til en sak hvor det er ukjent gjerningsmann og ingen knytning mellom offer og gjerningsmann.

Trafikkdata fra offerets telefon er ofte viktig i drapssaker. De gir objektive holdepunkter for offerets bevegelser i tiden før drapet og hvem offeret har vært i kontakt med. Dette kan i mange tilfeller gi opplysninger om hvem som var offerets nærmeste bekjente, og dermed viktige vitner for etterforskningen. Videre vil det kunne gi opplysninger om et mulig motiv og en mulig gjerningsmann.

[7] Brev av 08.12.09 fra Post- og teletilsynet til Justis og politidepartementet, PT-ref 0906631-2 og høringsnotatet pkt 2.5, s 19
[8] Se pkt 3.3

I saker med kjent gjerningsmann vil trafikkdata fra mistenktes telefon være med på å bekrefte eller avkrefte mistenktes forklaring, avdekke ytterligere impliserte mv.

Den største utfordringen er likevel når gjerningsmannen er ukjent og det ikke foreligger noe åpenbart motiv. I disse sakene er de stedsspesifikke sporene av stor betydning. Basestasjonsutskrifter er et slikt viktig spor. Det er avgjørende for etterforskningen å finne ut hvem som har vært i nærheten av åstedet i tiden for drapshandlingen. Dette gir opplysninger både om viktige vitner og mulig gjerningsmann.

Drapssaker - noen sakseksempler;

Drosjedrapet (1999). En drosjesjåfør ble funnet skutt og drept på en avsidesliggende gårdsvei i Nittedal i januar 1999. Trafikkdata fra offerets telefon viste kontakt med en av de mistenkte i timene før drapet. Trafikkdata fra mistenktes telefon knyttet ham direkte til drapshandlingen og avdekket ytterligere en mistenkt i saken. Det forelå ikke noe logisk motiv og det var heller ingen klar knytning mellom offer og gjerningsmenn. Begge de mistenkte ble dømt, og trafikkdata var helt avgjørende for utfallet.

Orderud-saken (1999). Tre personer ble drept på Orderud-gård i mai 1999. Fire personer ble pågrepet i juni 1999 og senere domfelt for medvirkning til drap. Trafikkdata var et av flere viktige bevis i saken. Det ble innhentet basestasjonsutskrifter for å kartlegge aktiviteten i området rundt åstedet, og trafikkdata fra de mistenktes telefoner ble sentralt for etterforskningen, blant annet for kontroll av de mistenktes forklaringer og kartlegging av bevegelser. Saken viser også behovet for lengre lagringstid, idet viktige forberedelseshandlinger, blant annet anskaffelse av våpen, ikke kunne kontrolleres gjennom trafikkdata fordi disse delvis var tapt når politiet fikk kjennskap til hendelsen.

Baneheia-saken (2000). To små jenter ble voldtatt og drept i et friluftsområde i Kristiansand i mai 2000. Gjerningsmennene ble først pågrepet i september 2000. Det var ingen forbindelse mellom ofrene og gjerningsmennene. Basestasjonsutskrifter var viktige for å klarlegge aktiviteten rundt åstedet og for å identifisere gjerningspersonene. Trafikkdata fra de mistenktes telefoner var viktige for å klarlegge de mistenktes bevegelser i tiden rundt drapstidspunktet, og for å kontrollere deres forklaringer.

Førde-saken (2004). Ei jente ble funnet drept i Førde i Sogn sommeren 2004. Gjerningsmannen ble først identifisert etter ca 5 måneder etter en omfattende etterforskning hvor blant annet trafikkdata og andre stedsspesifikke spor ble analysert. Disse stedsspesifikke sporene var grunnlaget for en omfattende DNA-undersøkelse av nesten 1.400 personer som hadde vært i det aktuelle området på gjerningstidspunktet. Til slutt ble gjerningsmannen identifisert gjennom DNA-treff.

Nokas-saken (2004). Ran av Norsk Kontantservice i Stavanger sentrum og drap på politimann i april 2004. Ranet var nøye planlagt, men likevel var trafikkdata viktig i etterforskningen. Basestasjonsutskrifter gav opplysninger om både vitner i nærheten av åstedet, samt telefoner som gjerningsmennene hadde benyttet. Gjerningsmennenes telefoner var opprettet kun for å brukes til ranet ("ranstelefoner"). Telefonene gav likevel opplysninger om adkomst og fluktrute. Trafikkdata gav også viktig informasjon om forberedelseshandlingene (planleggingsfasen). I tillegg ble trafikkdata blant annet brukt i alibi-prosjektet for å sjekke personer "inn eller ut" av saken. I Nokas-saken ble også IP-adresser viktig for å identifisere internettkafeér og andre brukersteder for elektronisk kommunikasjon på Internett. Lokaliseringen og pågripelsen av David A. Toska var et direkte resultat av at IP-adressene for hans e-postbruk ble identifisert og sporet.

Drammen-saken (2007). En tidligere eks-torpedo fra Litauen ble dømt til 15 års fengsel for ran og drap av en 56-årig norsk sjømann i Drammen. Ved etterforskningen ble trafikkdata viktig både for å fastslå dødstidspunkt og for å kartlegge tiltaltes bevegelser. Tiltalte ble domfelt i Drammen tingrett, men så frifunnet av juryen i Borgarting lagmannsrett. Fagdommerne satte rettens kjennelse til side og saken ble senere behandlet av Borgarting lagmannsrett (stor meddomsrett). Fra den siste dommen[9] refereres: "*Rettsmedisinernes observasjoner samsvarer med observasjoner fra personell som kom til åstedet, og de støttes av utskrifter fra Bs telefon- og bankkortbruk*" og "*På bakgrunn av telefonutskrifter over hvilke basestasjoner*

[9] Borgarting lagmannsretts dom av 19.12.08 (LB-2008-61703)

As mobiltelefon har slått inn på, kan tidsrommet fastslås til mellom kl 20:06 og 20:49. Lagmannsretten legger til grunn at det er overveiende sannsynlig at voldsutøvelsen har funnet sted i dette tidsrom"

Follo-saken (2008). Drap av en person under særdeles skjerpende omstendigheter på Nesodden i Follo i juli 2008. Trolig var saken et internt oppgjør innen et litauisk prostitusjons- og hallikmiljø i Oslo-området. Fire personer er domfelt for drapet. Trafikkdata var viktig for å kontrollere de mistenktes kontaktnett, bevegelser og til kontroll av forklaringer.

Kongsvinger-saken (2009). En person ble funnet brutalt knivdrept i Kongsvinger i juli 2009. Offeret tilhørte et rusmiljø i Kongsvinger. Trafikkdata var viktig for å kartlegge bevegelser i nærheten avåstedet. Saken ble senere oppklart ved at offerets mobiltelefon ble tatt i bruk av gjerningsmannen. Trafikkdata var således meget viktig for å identifisere mistenkte. Saken er ikke rettskraftig.

Haugerud-saken (2009). En sentral person i gjengmiljøet i Oslo ble drept i en bil på Haugerud i Oslo i januar 2009. Politiets oppfatning er at drapet var utløst av en konflikt i gjengmiljøene i Oslo. Etterforskningen tyder på at drapet ble planlagt/avtalt gjennom en fiktiv Facebook-profil på internett. Trafikkdata knyttet til bestemte IP-adresser er av stor betydning for etterforskningen. Tiltale er foreløpig ikke tatt ut.

2.3.2 Saknetsaker

Etterforskning av saknetsaker er utfordrende for politiet. Innledningsvis er det vanskelig å si med sikkerhet om det dreier seg om et straffbart forhold eller om vedkommende har blitt borte frivillig.

En sentral undersøkelse i denne type saker er å kontrollere om saknedes telefon fortsatt er i bruk, eventuelt hvor den ble benyttet sist (trafikkdata). På samme måte sjekkes også andre personspesifikke elektroniske spor knyttet til saknede, eksempelvis bruk av bankkort, bombrikke i bil mv. På denne måten kan man få en viktig indikasjon på hvorvidt saknede fortsatt er i live, og hvor han/hun eventuelt oppholder seg.

Det kan av grunnene nevnt ovenfor gå ganske lang tid før det klarlegges om det er begått en straffbar handling, og eventuelt hvilken straffbar handling det er snakk om. Dette gjør at viktige trafikkdata kan gå tapt. Dersom det i verste fall viser seg at saknede er blitt drept, vil det være meget aktuelt å innhente stedsspesifikke spor (blant annet basestasjonsutskrifter) fra antatt drapsåsted. Utfordringen er å klarlegge nøyaktig gjerningssted og gjerningstidspunkt.

Dersom man ut fra disse undersøkelsene klarer å identifisere en gjerningsmann, vil personspesifikke spor for mistenkte være meget aktuelt å innhente på samme måte som i øvrige drapssaker. Problemet er at tiden da har gått og viktige data kan ha gått tapt.

Saknetsaker – noen eksempler;

Lena-saken (2005). Kvinne fra Lillesand forsvant fra Tananger utenfor Stavanger 3.mars 2005. Meldt saknet av familien ca en måned senere. Etterforskningen tydet på at saknede kunne ha foretatt samtaler like før hun ble borte. Når dette ble aktuelt å undersøke var trafikkdata slettet. (Dette var før bestemmelsen i strpl §215a ble innført). Eks-samboeren ble pågrepet for drapet i 2008. Offeret er aldri funnet. Han ble dømt til 19 års forvaring i 2010, men saken er ikke rettskraftig. Selv under hovedforhandlingen var de manglende trafikkdata et viktig tema. Post- og teletilsynet sa i sin tid nei til å gi politiet tilgang til trafikkdata for hennes mobiltelefon, da det ikke var dokumentert at en straffbar handling hadde funnet sted.

Dung Tran Larsen-saken (2007). En kvinne ble meldt saknet i Hordaland i juli 2007 av sin ektemann. Hun hadde da vært borte i ca 1 uke i følge ektemannen. Etterforskningen viser at siste observasjon av saknede var ca 1 måned før hun ble meldt saknet. Ektemannen og flere i hans familie ble siktet for

forsettlig drap og pågrepet. Trafikkdata både fra saknede og de mistenkte ble sentralt for etterforskningen. Saken ble etter 2 års etterforskning henlagt etter bevisets stilling. Saknede har ikke kommet til rette.

Faiza-saken (2010). En kvinne ble meldt saknet fra Bærum. Hun var kidnappet av en ukjent gjerningsmann, og ringte politiet fra bagasjerommet på gjerningsmannens bil. Kvinnen ble senere funnet drept. To personer er pågrepet. Trafikkdata er viktig for å sjekke offerets kontaktnett og bevegelser i forkant av kidnappingen og drapet. Trafikkdata fra de mistenktes telefoner står sentralt i arbeidet med å sjekke bevegelser. Saken er fremdeles under etterforskning.

2.3.3 Narkotikasaker

Narkotikasaker kjennetegnes av at det er få vitner til de straffbare forholdene. Det er skjult kriminalitet, og all befatning med narkotika er straffbar. Det betyr at de fleste som har viktig informasjon i saken som regel også er innblandet på ett eller annet vis. Sakene er derfor vanskelige å avdekke og oppklare.

Politiet har fått flere ulike metoder som etter bestemte vilkår kan brukes blant annet for å avdekke alvorlig narkotikakriminalitet, herunder kommunikasjonskontroll (avlytting av innhold i kommunikasjon), romavlytting, provokasjonslignende tiltak, hemmelig ransaking, beslag/utleveringspålegg med utsatt underretning til mistenkte. Dette er metoder som i all hovedsak er egnet når politiet driver proaktiv (skjult) etterforskning. De aller fleste narkotikasaker avdekkes likevel uten at det er noen skjult etterforskning i forkant (kun reaktiv etterforskning).

Gjennomgang av trafikkdata er et meget viktig etterforskningsskritt, både i proaktive og reaktive etterforskningsfaser. De fleste som driver med alvorlig narkotikakriminalitet er yrkeskriminelle. De vet hva politiet kan finne ut gjennom etterforskning, og tar forholdsregler mot dette[10]. Blant annet vet de at politiet vil undersøke telefontrafikk, enten gjennom avlytting eller ved gjennomgang av trafikkdata. De bytter derfor ofte telefonnummer og registrerer nummer på andre personer eller på fiktive identiteter. Derfor tar det ofte lang tid å klarlegge hvilke telefonnummer de mistenkte har benyttet.

Politiets fokus har de senere årene flyttet seg enda mer mot bakmennene, for å kunne ramme de som har den største profitten. Bakmennene er som oftest ikke i nærheten av narkotikaen, da dette er risikofylt. Trafikkdata er helt nødvendig for å identifisere og pågripe bakmennene for innførsel og omsetning.

Narkotikakriminaliteten er internasjonal. Dette betyr at norsk politi må samarbeide med utenlandske politimyndigheter for å avdekke bakmenn og kurerer. Dette samarbeidet er tidkrevende.

Narkotikakriminalitet – noen sakseksempler;

Kenwood-saken (2002). I forbindelse med en rutinekontroll beslagla politiet i Oslo ca 10kg amfetamin og 4kg kokain i juli 2002. Tre personer ble pågrepet. Det var ingen proaktiv etterforskning i forkant av beslaget. Avhør og gjennomgang av trafikkdata var de viktigste bevisene i saken. Dette medførte pågripelse av ytterligere fem personer, herunder flere norske bakmenn. Etterforskningen medførte at det ble tatt ut tiltale for et langt større kvantum enn beslaget. På dette tidspunktet var dette Norges største narkotikasak. Alle åtte personene ble dømt til lange fengselsstraffer.

[10] Se også pkt 1.2

Operasjon Broken Lorry (2006). Kripos avdekket i juni 2006 et marokkansk narkotikanettverk som opererte i hele Europa. I samarbeid med flere politidistrikter og andre lands politimyndigheter ble totalt 43 personer pågrepet, og det ble beslaglagt store mengder narkotika. Åtte av de pågrepne ble pågrepet i utlandet og utlevert til Norge. Det ble i denne saken foretatt proaktiv (skjult) etterforskning både i Norge og i Nederland. Historiske trafikkdata ble likevel helt avgjørende bevis for en rekke av de tiltalte. To av bakmennene som ble utlevert fra Nederland ble idømt 21 års fengsel. Det var første gang lovens maksimumsstraff ble brukt i en narkotikasak. Trafikkdata var helt sentrale bevis mot begge bakmennene. I den samme saken ble en av de norske mottakerne først identifisert 8 måneder etter at saken var rullet opp. Dette medførte at relevante trafikkdata var slettet.

Operasjon Green Lamp (2008). Politiet avdekket gjennom 2008 ca 50 ulike cannabisplantasjer i Norge. Det var personer av vietnamesisk opprinnelse som stod bak plantasjene, og trafikkdata ble avgjørende for å avdekke bakmenn og se sammenhenger mellom sakene. Ved å innhente trafikkdata fra de mistenktes telefoner kunne en sammenligne dataene og få opplysninger om hvem som organiserte opprettelsen og driften av plantasjene. Etter denne operasjonen er det ikke avdekket tilsvarende plantasjer i Norge, og politiet mener at problemet har forflyttet seg til andre land.

Operasjon Glatt Fisk (2008). Etterforskning foretatt av Kripos av et større norsk narkotikanettverk i 2007-2008 resulterte i flere store beslag av narkotika. Etterforskningen avdekket at en hovedmann i Norge kommuniserte med sine leverandører i utlandet via en web-basert e-posttjeneste. Beskjeder ble på denne måten utvekslet via internett. Sporing av IP-adresser var derfor sentralt for etterforskningen. Manglende lagring av IP-logger i Norge (kun 21 dager) ble en utfordring i saken. Saken er ikke rettskraftig.

Bolivia-saken (2008). Tre unge jenter ble pågrepet på flyplassen i Cochabamba på vei til Norge. I kofferten til en av jentene ble det funnet ca 22kg kokain. I forbindelse med etterforskningen i Bolivia ble det nødvendig å kontrollere de mistenktes forklaringer og undersøke hvem de hadde hatt kontakt med. I den forbindelse anmodet bolivianske myndigheter om trafikkdata fra de mistenktes telefoner i Norge. Trafikkdata fra norske telenett har vært av betydning for etterforskningen i Bolivia. Det er tatt ut tiltale i saken, men den er foreløpig ikke behandlet i rettssystemet.

Narkotikasak Sunnhordland (2008). I en narkotikasak i Sunnhordland i 2008 viste etterforskningen at siktede i all hovedsak benyttet internett til å kommunisere med sine leverandører og selgere. Saken var utfordrende idet mistenkte benyttet et sammensurium av bredbånd, trådløse nett og mobile bredbåndsmodem. Relevante IP-data kunne gitt viktig informasjon om siktedes distribusjonsnett, men den korte lagringstiden (21 dager) gjorde at dette ikke lykkes.

Operasjon Andromeda (2009). Kripos etterforsket i samarbeid med en rekke politimyndigheter i Europa et meget omfattende albansk narkotikanettverk. Etterforskningen resulterte i flere store narkotikabeslag flere steder i Europa. Trafikkdata er viktig i saken da de mistenkte byttet telefonnummer hyppig og fordi alle nummer av denne grunn ikke ble avlyttet. Videre ble det avdekket at flere av de mistenkte avtalte å utveksle viktig informasjon via MSN og Skype på internett. Noen av disse chatloggene ble senere funnet på beslaglagte pc'er, men manglende muligheter for sporing av IP-adresser i Norge ble et problem. I forbindelse med en av delsakene som omhandlet beslag av 9kg heroin i Sarpsborg i mai 2009 ble trafikkdata avgjørende for domfellelse av flere av de tiltalte[11]. Saken er ikke rettskraftig.

2.3.4 Grove ran

Grove ran er som oftest kompliserte saker å etterforske da det ligger i sakens natur at det er ukjente gjerningsmenn. Stedsspesifikke spor som basestasjonsopplysninger er av stor betydning. Disse kan gi opplysninger både om rekognosering og gjennomføring av ran, samt avdekke hvilke potensielle vitner som var i samme område på de aktuelle tidspunktene.

[11] Oslo tingretts dom av 25.03.10, s 10 flg (09-2004471MED-OTIR/08). Dommen baserer seg i stor grad på analyse av de tiltaltes bevegelser basert på trafikkdata innhentet i Norge og Sverige sammenholdt med deres forklaringer. Trafikkdata var avgjørende både for å klarlegge de faktiske bevegelsene forut for beslaget, samt for å sjekke holdbarheten av de tiltaltes forklaringer. Det var nødvendig å innhente ytterligere trafikkdata under hovedforhandlingen. Trafikkdata var slettet hos de norske teleoperatørene, men fordi deler av hendelsesforløpet hadde funnet sted i Sverige var det mulig å innhente trafikkdata hos de svenske teleoperatørene som har 1 års lagringspraksis.

Store og alvorlige ran er som regel utført av godt organiserte miljøer. Etterforskningen av slike saker tar derfor lang tid og informasjonen kommer frem underveis. I etterforskningen av Nokas-ranet ble to av de som nå er domfelt først pågrepet etter 9 måneders etterforskning. Dette er et eksempel på at sentral informasjon ofte tilflyter politiet så sent i etterforskningen at trafikkdata er slettet selv når politiet bruker alle sine ressurser.

Felles for organisert kriminalitet er at aktørene er godt organiserte og erfarne kriminelle. De gir sjelden forklaring til politiet under etterforskningen, men avventer til de er forelagt alle bevisene og avgir sin forklaring først under hovedforhandlingen. Det betyr at opplysningene om angivelige bevegelser og angivelige telefoner først kommer på et tidspunkt hvor teledata er slettet, og da blir det langt vanskeligere for politiet å kontrollere forklaringen. Dermed blir det også vanskeligere for domstolen å få saken tilstrekkelig opplyst.

Grove ran av verditransporter og finansinstitusjoner var utbredt på 90-tallet og frem til Nokas-saken i 2004. Etter dette har denne typen ran avtatt. De grove ranene de siste årene har i større grad vært ran av butikker, kiosker osv. Disse synes å være mindre planlagte.

Nokas-saken gis som eksempel under sakstypen drapssaker tidligere i dette notatet, selv om tiltalen gjaldt grovt ran med døden til følge.

2.3.5 Seksuelle overgrep

Seksuelle overgrep omfatter mange ulike sakstyper med ulike utfordringer. En stor andel av sakene hvor offer og gjerningsmann kjenner hverandre ender opp med å bli en vurdering av om retten tror på offer eller gjerningsmann, i mangel av objektive bevis. Trafikkdata er i mange tilfeller godt egnet til å kontrollere de implisertes forklaringer med hensyn til kontaktmønster og bevegelser.

I saker med ukjent gjerningsmann, eksempelvis overfallsvoldtekter, er de stedsspesifikke sporene viktige da dette gir en oversikt over hvem som har befunnet seg i nærheten av åstedet på gjerningstidspunktet. I saker med lignende modus er det da mulig å sammenligne de stedsspesifikke sporene for å se om det kan være samme gjerningsmann.

Et annet aspekt ved sedelighetssakene er at overgrepets traumatiserende art ofte medfører at fornærmede bruker lang tid før hendelsen anmeldes. Særlig er dette fenomenet velkjent når barn er ofre. Når anmeldelsen kommer kan teledata allerede være slettet, ikke minst fordi flere og flere av overgrepene mot barn skjer etter initiell kontakt over internett hvor langringstiden av trafikkdata kun er 21 dager. Lengre lagringstid av trafikkdata ville lettet avsløringen av overgripere, selv i de tilfellene hvor barnet bruker noen måneder på å bearbeide opplevelsen.

Seksuelle overgrep – noen sakseksempler;

> *Lommemannsaken (2008).* Saken dreier seg om en lang rekke overgrep mot barn over en lang periode. Det er den første seriesaken av dette slaget i Norge. Politiet kartla ca 300 ulike straffbare forhold med tilsvarende modus. I de fleste av sakene var det ikke innhentet stedsspesifikke spor når saken ble anmeldt, og det var derfor vanskelig å undersøke sammenhenger mellom disse sakene, blant annet om det var noen personer som gikk igjen i nærheten av de ulike åstedene. Etter hvert hadde politiet ca 1.000 aktuelle kandidater som måtte sjekkes i et alibi-prosjekt (tidligere domfelte for seksuelle overgrep og personer som hadde befunnet seg i nærheten av flere av åstedene). I januar 2008 ble en

Bergensmann pågrepet da DNA-treff viste at han var den omtalte "Lommemannen". Kort lagringstid på trafikkdata og manglende innhenting av stedsspesifikke spor (basestasjonsutskrifter) når sakene ble anmeldt gjorde at politiet måtte innhente andre typer stedsspesifikke spor som utskrifter av alle betalingsterminaler, opplysninger om bruk av tippekort fra Norsk tipping, bompasseringer mv. i nærheten av åstedene. Disse var fortsatt tilgjengelige for en del av de straffbare forholdene. Lengre lagringstid av trafikkdata ville medført at en rekke av de aktuelle forholdene langt enklere kunne vært sjekket inn eller ut av saken. Saken viser utfordringene med seriesaker og manglende lagring av trafikkdata.

Operasjon Buddy (2007). Etterforskningen startet ved at politiet mottok voldtektsanmeldelse mot en 32-årig mann fra Rogaland. Ved ransaking fant politiet en stor mengde overgrepsmateriale mot barn på mannens PC, herunder bilder og filmer han selv hadde produsert ved å gjøre opptak av samtaler han hadde hatt med jenter i alderen 9-16 år via MSN Messenger mens webkamera var tilkoblet, og mens han instruerte jentene til å foreta seksuelle handlinger foran kamera. To av jentene hadde han også møtt og hatt samleie med. Det var en omfattende jobb å identifisere de fornærmede, og sporing av IP-adresser stod sentralt. Ved å gjennomgå kontaktlistene på mistenktes e-postkonto , sammenligne disse med kontaktlister hos fornærmede og deretter spore aktuelle IP-adresser, avdekket politiet også at flere voksne menn hadde begått overgrep mot noen av de samme jentene. 32-åringen ble dømt i Høyesterett[12] til fengsel i 5 år 6 måneder. Dommen omfattet internettrelaterte seksuelle overgrep mot 46 jenter, i tillegg til seksuell omgang med to av dem. En av de andre tiltalte ble dømt[13] til fengsel i 2 år 1 mnd hvorav 1 år betinget. Vedkommende ble identifisert gjennom trafikkdata fra mobiltelefon. Om tiltaltes mobiltelefonbruk bemerket lagmannsretten følgende: "*Når det gjelder den beslaglagte mobiltelefon vises til den fremlagte loggutskrift som viser hyppig kontakt mellom D og domfelte. Lagmannsretten legger til grunn at mobiltelefonene var et viktig verktøy for domfelte når han skulle etablere det tillitsforhold til D som senere gjorde det mulig for ham å oppnå seksuell omgang med henne*".

Gruppevoldtekt Oslo (2005). Fem personer domfelt for grov gruppevoldtekt av ei 16 år gammel jente. Trafikkdata var av stor betydning for å klarlegge om flere av de tiltalte hadde vært på åstedet, og for å kontrollere troverdigheten av deres forklaringer. Alle 5 personene ble domfelt i både Oslo tingrett og Borgarting lagmannsrett. Oslo tingrett bemerker om tiltalte E: "*Retten legger her særlig vekt på at G utpekte ham, at han var venn av den nå etterlyste, at mobiltelefonutskriften viser at han var i Oslo sentrum i den relevante tidsperioden og da hadde kontakt med den nå etterlyste og F samt at han var i –området fra ca kl 1800*". For tiltalte A bemerker retten: *"… Derimot legger retten til vekt på mobiltelefonutskriften der ringemønsteret for dagene rundt overgrepsviser at der er A som har brukt telefonen. Utskriftene viser at han kom til –området ca kl 2148 som er i den perioden da overgrepene fant sted…"*[14]

2.3.6 Internettrelaterte seksuelle overgrep

Internett har gitt nye muligheter og arenaer for seksuelle overgrep. Dette kan være alt fra kontaktetablering mellom overgriper og offer i sosiale medier på internett ("grooming") til formidling av grove seksuelle overgrep live via webkamera. I tillegg gir internett en stor mulighet for spredning av foto/videomateriale av seksuelle overgrep, eksempelvis filmer av seksuelle overgrep som spres gjennom lukkede forum eller åpne fildelingsnettverk.

Denne typen saker har flere særegenheter. For det første er politiet helt avhengig av å kunne spore tilbake til hvem som faktisk kommuniserer, det vil si at man må kunne knytte IP-adresser til bestemte personer eller steder. Det andre er at internett er grenseløst, og at kommunikasjon enkelt kan gå på tvers av landegrenser. Dette krever at politiet løser sakene gjennom internasjonalt samarbeid, hvilket er tidkrevende. Politiet må som oftest jobbe "bakover" i kjeden for å kunne identifisere ofre og produsenten av overgrepsmateriale. Disse prosessene tar tid, og i mellomtiden går IP-logger tapt.

[12] Norges Høyesteretts dom av 6.februar 2009
[13] Agder lagmannsretts dom - LA-2008-49154
[14] Oslo tingretts dom 01.12.05 (TOSLO-2005-129056) og Borgarting lagmannsrettsdom av 19.05.06 (LB-2006-216), samt www.aftenposten.no/nyheter/iriks/article3569530.ece

Norge har med dagens praksis hvor IP-logger kun lagres i 21 dager meget begrenset mulighet for å kunne avdekke både overgripere og personer som sprer overgrepsmateriale med base i Norge. Norge er i ferd med å bli en frihavn for denne typen kriminelle.

Anslagsvis to ganger i måneden mottar Kripos informasjon fra kolleger i utlandet om overgrepssaker hvor nordmenn er involvert. Problemet er at 21-dagersfristen er utløpt før Kripos mottar informasjon om konkrete IP-adresser fra internasjonale kollegaer. Kripos får stadig opplysninger om nordmenn som deler overgrepsmateriale over nettet. Bevisene er sterke, men gjeldende sletteprakis gjør informasjonen ubrukelig for etterforskerne.

Gjennom tjenesten *tips.kripos.no* mottar Kripos regelmessig henvendelser om mulig pågående overgrep, hvor etterforskningen ikke kommer videre på grunn av at IP-historikken slettes nesten umiddelbart av noen teletilbydere (ISP'er).

Ved å ha et regelverk som gjør at man i praksis ikke klarer å etterforske og iretteføre disse forbrytelsene klarer ikke Norge å oppfylle de internasjonale forpliktelsene vi har gjennom blant annet FNs barnekonvensjon artikkel 34[15]. I realiteten innebærer dette at Norge jevnlig bryter FNs barnekonvensjon. Datalagringsdirektivet vil utvilsomt bidra til en forbedring på dette området.

Internettrelaterte seksuelle overgrep – noen sakseksempler;

> *Sak 1 (2009).* I forbindelse med en politiaksjon i Mellom-Europa i juni 2009 fikk Kripos oversendt 709 unike, norske IP-adresser som var benyttet til å utveksle overgrepsmateriale (mot barn). Det betyr at mange personer i Norge har mottatt eller sendt filer med overgrepsmateriale på dette nettverket. På grunn av manglende lagring av trafikkdata var det ikke mulig å iverksette etterforskning mot mistenkte i Norge.
>
> *Sak 2 (2009).* I begynnelsen av oktober 2009 fikk Kripos oversendt tilsvarende IP-adresser fra brasiliansk politi i forbindelse med en aksjon mot et nettverk for distribusjon av overgrepsmateriale der det var blitt utvekslet filmer av overgrep mot barn. Som følge av dette ble blant annet 121 personer arrestert i Spania. På grunn av manglende lagring av trafikkdata var det ikke mulig å iverksette etterforskning mot mistenkte i Norge.
>
> *Sak 3 (2006).* En 42 år gammel mann fra Bergen opprettet kontakt med mindreårige gutter via ulike nettsamfunn. Når han chattet med guttene utga han seg for å være jevnaldrende med dem. Han avtalte møter med flere av de fornærmede. En av disse, en da 15-årig gutt som hadde avtalt å møte overgriperen på torget i Bergen, ante imidlertid uråd da han forstod at den han møtte var betydelig eldre enn han hadde utgitt seg for å være, og kontaktet politiet. Domfelte ble identifisert gjennom sporing av IP-adressen han hadde operert fra i sin kontakt med 15-åringen. Ved å undersøke hvilke andre IP-adresser domfeltes IP-adresse hadde vært i kontakt med klarte politiet etter hvert å identifisere flere ofre. 42-åringen ble i januar 2010 dømt til 10 års forvaring med en minstetid på 6 år. Han ble i tillegg dømt til å betale erstatning til 11 av ofrene.

2.3.7 Vinningskriminalitet

Vinningskriminaliteten har endret seg de siste årene fra stort sett "lokale" gjerningsmenn, til stor grad av omreisende kriminelle. Store deler av vinningskriminaliteten har blitt mer organisert og profesjonalisert. Utenlandske organiserte grupperinger dominerer blant gjerningsmennene.

---

[15] NOU 2009:15 – "Skjult informasjon – åpen kontroll", s 194: "
Etter FNs barnekonvensjon artikkel 34 er konvensjonspartene forpliktet til å beskytte barn mot alle former for seksuell utnytting og seksuelt misbruk. For dette formål skal partene særlig treffe alle egnede nasjonale, bilaterale og multilaterale tiltak for å hindre at noen tilskynder eller tvinger barn til å delta i enhver form for ulovlig seksuell aktivitet, utnytter barn ved å bruke dem til prostitusjon eller andre ulovlige seksuelle handlinger eller utnytter barn ved å bruke dem i pornografiske opptredener eller i pornografisk materiale. Barnekonvensjonen er inkorporert i norsk lov gjennom menneskerettsloven 21. mai 1999 nr. 30."

Gjennomgang av trafikkdata for mistenkte personer sammenholdt med modus vil kunne knytte mistenkte til flere grove tyverier av samme art.

For å kunne se sammenhenger mellom denne typen straffbare forhold er de stedsspesifikke sporene sammenholdt med modus av stor betydning. Det vil vise om de samme gjerningsmennene går igjen på flere forhold. Trafikkdata fra de konkrete numrene til gjerningsmennene vil kunne bidra til å identifisere både gjerningsmennene og bakmannsapparatet.

Mobil vinningskriminalitet er et prioritert satsningsområde for politiet, som det også har vært stor oppmerksomhet rundt i media den senere tiden. Tilgang til historiske trafikkdata er helt avgjørende for at Kripos og politidistriktene skal være i stand til å bekjempe mobile vinningskriminelle.

Vinningskriminalitet – noen sakseksempler:

> *Op Elektro (2006).* Store deler av Sør-Norge var utsatt for en rekke grove tyverier (”sjokkbrekk”) fra store elektronikkbutikker. Modus syntes å være meget lik i en rekke av sakene. Stedsspesifikke spor som basestasjonsutskrifter og trafikkdata fra konkrete mistenkte ble benyttet for å se sammenhenger mellom sakene. Det ble avdekket tre ulike kriminelle nettverk som stod bak ca 40 grove tyverier.
>
> *Urmakersakene (2009).* En utenlandsk tyveribande ble pågrepet i Haugesund etter et grovt tyveri fra en urmaker (”sjokkbrekk”). Modus var den samme som på flere andre steder i landet. Trafikkdata ble viktig for å knytte gjerningsmennene til andre forhold. Gjerningsmennene ble dømt for tilsvarende forhold både i Kongsberg, Stavanger og Haugesund. Totalt ble det stjålet kostbare klokker for ca 4,6 millioner kroner. Saken er ikke rettskraftig.
>
> *Op Pink BMW (2009).* Kripos etterforsket høsten 2009 et profesjonelt serbisk rans- og tyverinettverk som opererte i Norge. Etterforskningen dreide seg opprinnelig om mulig tilslag mot en bedrift, men gjennom skjult etterforskning ble det avdekket at de mistenkte var i ferd med å gjennomføre et grovt tyveri fra en bolig, og gjerningspersonene ble pågrepet. Den etterfølgende gjennomgangen av trafikkdata fra flere av medhjelperne har avdekket at disse knyttes til et hundretalls grove tyverier på Østlandsområdet. Uten trafikkdata ville knytningen til disse forholdene ikke latt seg påvise. Saken er ikke rettskraftig.

2.3.8 Datakriminalitet

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 og trusler og sjikane over internett. I de fleste sammenhenger blir dette omtalt som datakriminalitet. Datakriminalitet skiller seg fra andre sakstyper ved at den kriminelle handlingen foregår på det elektroniske mediet selv (”subject in the crime”).[16]

Det som særlig kjennetegner denne typen saker er at politiet står uten andre potensielle bevis enn de som finnes i de digitale mediene og kildene. Internett er i utgangspunktet uten vitner og fysiske eller håndfaste spor. Etterforskning av datakriminalitet vil som regel alltid handle om å søke etter spor i de dataene som er lagret og logget i tilknytning til handlingen. På grunn av den teknologien internett er basert på, vil disse sporene i siste instans nesten alltid være knyttet til en IP-adresse.

[16] Se også NOU 2009:15, pkt 8.6.4, s 82-82, ”Datakriminalitet”

Litt forenklet kan man si at enhver datamaskin som brukes på internett er identifisert ved sin IP-adresse[17]. Det er derfor en forutsetning for all reaktiv etterforskning av datakriminalitet at en kan spore og identifisere en korrekt abonnent tilknyttet en IP-adresse, for derav å kunne identifisere en gjerningsmann.

Internett er grenseløst, og det er i praksis ingen begrensninger i hvorfra eller mot hvem datakriminalitet kan utøves. De som utøver og profitterer på denne typen kriminalitet utnytter selvsagt dette. Det er en sterk erkjennelse blant politiorganisasjoner i alle land at etterforskning og bekjempelse av datakriminalitet forutsetter utstrakt internasjonalt politisamarbeid. Som tidligere omtalt er slike prosesser tidkrevende, noe som forsterker behovet for lagring på samme måte som for andre sakstyper.

Datakriminalitet – noen sakseksempler:

> *Tele2-saken (2007).* Teknisk kompetente gjerningspersoner utviklet et lite dataprogram for å misbruke en kontrollfunksjon i forbindelse med Tele2 sin internettbaserte løsning for å bestille mobiltelefonabonnement. Gjennom å kjøre dette programmet lyktes gjerningspersonene å liste ut personnummer til anslagsvis 60.000 norske borgere, med senere potensial for utstrakt ID-misbruk. Som en del av en langvarig etterforskning, ble knytningen mellom IP-adresser og abonnenter avgjørende for å spore opp gjerningsmennene. IP-adressen ledet til flere brukere, og ytterligere etterforskning,blant annet analyse at beslaglagte datamaskiner, ga ytterligere spor. To personer er dømt i tingretten. Sakene er ikke rettskraftige.
>
> *Nettbanksakene (2006-2007).* Over en periode i årsskiftet 2006-2007 ble en rekke norske banker og bankkunder utsatt for urettmessig uttak av penger ved bruk av det som blir kalt en nettbank-trojaner. En langvarig og teknisk krevende etterforskning ble igangsatt ved Kripos, og innbefattet over 50 enkelttilfeller. I tillegg ble et ukjent antall saker overført politidistriktene for etterforskning. Sporing av IP-adresser stod helt sentralt, knyttet til alle ledd i utøvelsen av bedrageriene.
>
> *Photobucket (2008).* En av erdens største nettbaserte bildedelingstjenester Photobucket anmeldte et tilfelle av datainnbrudd og tyveri av brukerdata for i alt 66 millioner brukere fra hele verden, hvorav ca 120 000 norske. Innbruddet ble foretatt fra en norsk IP-adresse, som bl. a gjennom tjenestetilbyder ble knyttet til tiltalte i saken. Videre etterforskning avdekket ytterligere 187 enkelttilfeller av datainnbrudd på private e-postkontoer. IP-adresser var identifikatoren for alle sakene. Det foreligger tiltale i saken, men saken er ikke behandlet i domstolen.

2.3.9 Ulykkesetterforskning

Politiet etterforsker også ulykker, jfr strpl §224, 4.ledd. I disse tilfellene foreligger det ofte ikke mistanke om noe straffbart forhold, og da heller ikke skjellig grunn til mistanke mot noen bestemt person, men samfunnet har behov for å finne ut av årsaken til ulykken uavhengig av om noen kan stilles til ansvar for den.

I flere slike tilfeller vil det være aktuelt å undersøke trafikkdata, både for å fastslå tidspunkter i et hendelsesforløp ved å sammenholde trafikkdata opp mot vitners forklaringer.

Ulykkesetterforskning – et eksempel:

> *Godsvognulykken (2010).* I mars 2010 ble Oslo utsatt for en alvorlig ulykke etter at flere godsvogner kom i bevegelse og forflyttet seg ukontrollert fra Alnabru til Sjursøya i Oslo, en strekning på ca 7km. Spørsmålet om årsaken til ulykken ble umiddelbart et tema, men også hva som var gjort for å redusere skadene etter at det ble oppdaget at togvognene var i bevegelse. I denne forbindelse ble

[17] Noen ganger vil flere datamaskiner kunne opptre bak én IP-adresse, men i tilknytning til data som er ment lagret etter DLD vil dette i det alt vesentlige være innenfor samme husstand

> spørsmål om tidspunkt for varsling fra togsentralen og fra akuttsentralene et relevant tema. I slike saker foreligger det ofte ikke skjellig grunn til mistanke om et straffbart forhold mot enkelt personer, men det kan likevel være av stor samfunnsmessig relevans å innhente trafikkdata for å klarlegge de faktiske hendelsene. Etterforskningen pågår fortsatt.

Av påtaleinstruksen §7-4 fremgår det at det ved brann og ulykke som har voldt alvorlig personskade eller betydelig ødeleggelse av eiendom skal det iverksettes etterforskning selv om det ikke er grunn til mistanke om straffbare forhold. Samfunnet har et stort behov for en best mulig klargjøring av de faktiske forhold rundt alvorlige ulykker som for eksempel luft- og skipsfartulykker. Når politiet etterforsker slike saker vil beslag og utlevering være relevante virkemidler, og det bør også være adgang til å sikre trafikkdata uavhengig av krav til skjellig grunn til mistanke.

2.3.10 Oppsummering – politiets bruk av trafikkdata

Oppsummeringsmessig viser gjennomgangen av politiets bruk av trafikkdata at denne typen data er et nødvendig bevismiddel i mange ulike sakstyper, både de som berører enkeltpersoner og de som berører samfunnet som helhet.

Videre viser beskrivelsen at etterforskning er en dynamisk prosess hvor behovet for trafikkdata i mange saker ikke er avdekket før etterforskningen har pågått en stund. Politiets etterforskning er i hovedsak reaktiv, og en må derfor forsøke å rekonstruere hva som faktisk har skjedd for å finne ut hvem som eventuelt skal stilles til ansvar for dette. Trafikkdata er i disse tilfellene en av få objektive og kontrollerbare bevis.

På bakgrunn av faktum i de sakene det er referert fra ovenfor, er det også lett å tenke seg at resultatet ville vært annerledes dersom muligheten til å innhente trafikkdata ikke hadde vært til stede. Denne muligheten vil i nærmeste fremtid opphøre som følge av at faktureringsbehovet opphører. Innføringen av datalagringsdirektivet er viktig for (fortsatt) å drive en effektiv kriminalitetsbekjempelse, samt for å ivareta politiets oppgaver innen blant annet ulykkesetterforskning og søk etter saknede personer

DEL III - Trafikkdata – omfang og nytteverdi

3.1 Politiets bruk av trafikkdata - omfang

Kripos har innhentet statistikk[18] fra Telenor og NetCom som viser politiets bruk av trafikkdata i perioden 2007-2009.

Tallene viser at politiet innhentet ca 4.600 - 5.000 utskrifter pr år fra konkrete telefonnummer i denne perioden.

Når det gjelder utskrifter fra basestasjoner (stedsspesifikke spor) så ble dette innhentet i ca 250 tilfeller i 2007 og ca 300 tilfeller i 2008 og 2009.

Tall fra Post- og teletilsynet[19] viser at antall anmodninger om fritak fra taushetsplikt i perioden fra 2004 – 2008 har ligget jevnt på ca 1.800-1.900 pr år. Hver enkelt anmodning kan inneholde mer enn ett telefonnummer.

---

[18] Statistikk innhentet hos Telenor og NetCom februar 2010. Sakene omfatter både utskrifter basert på fritak fra Post- og teletilsynet, kjennelse fra retten, samtykke fra abonnent og utskrifter med hjemmel i KK-bestemmelsene (strpl §216b)

[19] NOU 2009:15 – Skjult informasjon – åpen kontroll, s 126

Post- og teletilsynet har i brev til Justis- og Politidepartementet[20] opplyst at de ikke har noen statistikk over hvilke straffebud politiet påberoper seg ved begjæring om fritak fra taushetsplikten, men at hovedtyngden av sakene dreier seg om *narkotikalovbrudd* (strl §162), *vinningskriminalitet* (strl §147, §§257-258) og *voldskriminalitet*.

Trafikkdata brukes altså i et stort antall alvorlige straffesaker hver eneste dag.

3.2 Nytteverdi av trafikkdata i etterforskningen

Politiet har åpenbart stor nytte av trafikkdata i etterforskningen. Det er likevel ikke gjort noen større undersøkelse for å se på nytteverdien av trafikkdata i forkant av høringsrunden.

Heller ikke i forbindelse med Metodekontrollutvalgets[21] rapport ble nytteverdien av trafikkdata undersøkt spesifikt, men utvalget antar at trafikkdata har vært til nytte i etterforskningen i ca 40% av sakene hvor trafikkdata er innhentet. De støtter seg til en tysk undersøkelse[22] fra 2008. Metodekontrollutvalget fant nyttegraden på 40% som tilfredsstillende.

Fra NOU 2009:15 – s 122 hitsettes:

> *Med tanke på at bruk av trafikkdata utgjør et betraktelig mindre inngrep i både mistenktes og berørte tredjepersoners personvern enn kommunikasjonsavlytting, og i lys av at metoden i hovedsak brukes i etterforskingen av alvorlig kriminalitet, finner utvalget at en nytteprosent på minimum 40 er tilfredsstillende.*

3.3 Kripos' undersøkelse

Kripos klare oppfatning er at nytteverdien av trafikkdata i etterforskning i Norge er langt høyere enn hva den tyske undersøkelsen viser. Kripos gjennomførte i mars 2010 en kvantitativ undersøkelse av bruk av trafikkdata i bestemte sakstyper.

Bakgrunnen for undersøkelsen var at det ikke er gjennomført noen måling av nytteverdien i forkant av høringsrunden. Beskrivelse av gjennomføringen og resultatene av undersøkelsen er inntatt i *vedlegg 1* til høringssvaret.

Undersøkelsen er begrenset til saker fra 2008 som har ført til en positiv påtaleavgjørelse. Forenklet sagt betyr det at etterforskningen er ferdig og at påtalemyndigheten har besluttet å ilegge en strafferettslig reaksjon.[23] Begrunnelsen for avgrensningen fremkommer i vedlegg 1.

Sakstypene som er undersøkt er;

- *Drap* (innbefatter strl §233 og legemsbeskadigelse med dødsfølge, jfr strl §229, siste straffealt.)
- *Grove narkotikasaker* (strl §162, 2. og 3.ledd)
- *Grove ran* (strl §268, jfr §267)
- *Seksuelle overgrep* (voldtekt, jfr strl §192, og seksuelle overgrep mot barn u/10 og 14 år, jfr strl§195)

Totalt sett utgjorde utvalget 1450 saker i 2008.

---

[20] Brev av 08.12.09 fra Post- og teletilsynet til Justis og politidepartementet, PT-ref 0906631-2
[21] NOU 2009:15: "Skjult informasjon – åpen kontroll", s 116-120
[22] Albrecht/Grafe/Kilchling 2008
[23] Saker hvor det er utferdiget forelegg eller påtaleunnlatelse, eller det er besluttet å bringe saken inn for retten med siktelse eller tiltale.

Undersøkelsen ble foretatt ved at det ble sendt et strukturert spørreskjema til registrert etterforsker ved hjelp av verktøyet Questback. I de tilfellene det ikke var registrert noen etterforsker, ble spørsmålene sendt til påtaleansvarlig.

Undersøkelsen ble gjennomført i perioden 03.03.10 – 12.03.10. Svarprosenten var 67%.

3.3.1 Bruk av trafikkdata

Alle respondentene fikk spørsmål om hvorvidt det var innhentet trafikkdata i den aktuelle saken.

Ble det innhentet historiske trafikkdata i forbindelse med etterforskningen av denne saken?

	Ja, mobil-/fasttelefoni	Ja, Ip-trafikk	Ja, både tlf og IP	Nei
Samlet - alle kategorier	**48,8 %**	**0,3 %**	**2,8 %**	**48,1 %**
Drap	73,9 %	0,0 %	0,0 %	26,1 %
Grove narkotikasaker	57,0 %	0,3 %	2,2 %	40,4 %
Grove ran	34,0 %	0,0 %	4,0 %	62,0 %
Seksuelle overgrep	23,9 %	0,5 %	4,6 %	71,1 %

Tallene viser at det i over halvparten av de undersøkte sakene (ca 52%) ble innhentet trafikkdata.

For de som opplyste at de ikke hadde innhentet trafikkdata i den aktuelle saken, ble det stilt følgende tilleggsspørsmål:

Hvorfor ble det ikke innhentet trafikkdata i denne saken?

	Ikke vurdert	Vurdert, men ikke nødvendig	Vurdert, men for kostbart	Vurdert nødvendig, men data slettet	Annet
Samlet - alle kategorier	**19,4 %**	**64,5 %**	**1,9 %**	**2,6 %**	**11,6 %**
Drap	33,3 %	66,7 %	0,0 %	0,0 %	0,0 %
Grove narkotikasaker	13,6 %	65,6 %	3,3 %	0,7 %	16,8 %
Grove ran	25,8 %	71,0 %	0,0 %	3,2 %	0,0 %
Seksuelle overgrep[24]	27,7 %	61,3 %	0,0 %	5,8 %	5,2 %

Resultatene viser at hovedårsaken til at trafikkdata ikke blir innhentet i en del saker er fordi det *ikke er nødvendig* (64,5%). Dette viser at det gjøres en hensiktsmessighetsvurdering før trafikkdata innhentes.

[24] For kategoriene som omhandler seksuelle overgrep, og hvor overgrepet har skjedd via internett, er det Kripos som i hovedsak innhenter trafikkdata fra tilbyderne før sakene sendes til politidistriktene. Dette utgjør ikke en stor andel saker, men vil kunne påvirke svarene fra etterforsker hvorvidt (ytterligere) trafikkdata var nødvendig å innhente.

Samtidig viser tallene at det i de sakene hvor trafikkdata ikke innhentes, skyldes det sjeldent at trafikkdata er *slettet* (2,6%). Det kan forstås slik at lagringstiden i liten grad er et problem i saker hvor det pr i dag ikke innhentes trafikkdata, men som likevel lar seg oppklare. Det er all grunn til å tro at resultatet ville vært høyere om undersøkelsen også omfattet henlagte saker. Men resultatene i pkt 3.3.4 viser at lagringstiden har en betydning i sakene hvor det i dag innhentes trafikkdata, se nedenfor.

3.3.2 Nytteverdi

For de som opplyste at de innhentet trafikkdata ble det stilt følgende tilleggsspørsmål:

Hvor enig eller uenig er du i at trafikkdata bidro med informasjon av stor betydning for etterforskningen i denne saken?

	Helt enig	Litt enig	Verken enig eller uenig	Litt uenig	Helt uenig
Samlet - alle kategorier	**60,7 %**	**21,8 %**	**5,6 %**	**3,4 %**	**8,6 %**
Drap	58,8 %	17,6 %	5,9 %	5,9 %	11,8 %
Grove narkotikasaker	63,7 %	20,4 %	4,7 %	2,2 %	9,0 %
Grove ran	57,9 %	26,3 %	5,3 %	0,0 %	10,5 %
Seksuelle overgrep	42,9 %	30,2 %	11,1 %	11,1 %	4,8 %

Tallene viser at *ca 82%* av de som innhentet trafikkdata var "*helt enig*" (60,7%) eller "*litt enig*" (21,8%) i at dataene hadde stor betydning for etterforskningen. I dette ligger det en politifaglig vurdering av at opplysningene hadde betydning. Hvilken betydning fremkommer nedenfor.

Resultatet for de spesifikke kategoriene viser at betydningen er noe ulik, men at summen av "*helt enig*" og "*litt enig*" ikke for noen kategorier er under *73%*. Dette viser etter Kripos oppfatning at trafikkdata er viktig i de tilfellene de innhentes.

For å undersøke *hvilken* nytteverdi trafikkdata hadde i de tilfellene de ble innhentet ble alle som opplyste at de innhentet trafikkdata bedt om å angi hva dataene ble benyttet til.

Dersom trafikkdata hadde betydning for etterforskningen i denne saken, hvilke opplysninger bidro det med? (flere svar mulig)

	Samlet - alle kategorier	Drap	Grove narkotikasaker	Grove ran	Seksuelle overgrep
Kontroll av mistenkte/siktedes bevegelser	**81,8 %**	92,3 %	87,6 %	87,5 %	34,8 %
Kontroll av opplysninger fremkommet i politiavhør eller andre undersøkelser	**76,8 %**	100,0 %	76,9 %	62,5 %	73,9 %
Opplysninger om mistenktes/siktedes kontaktmønster (kontaktanalyse)	**75,3 %**	38,5 %	80,8 %	50,0 %	54,3 %
Identifisering av gjerningsperson(er)	**54,2 %**	15,4 %	60,7 %	50,0 %	19,6 %
Sjekke personer inn/ut av saken	**39,5 %**	30,8 %	39,9 %	50,0 %	34,8 %

Kartlegge personer i et bestemt område (basestasjonsutskrifter)	**34,6 %**	30,8 %	37,3 %	68,8 %	4,3 %
Trafikkdata var ressursbesparende for saken ved at andre metoder/undersøkelser kunne utelates	**25,7 %**	38,5 %	26,6 %	31,3 %	13,0 %
Annet	**4,8 %**	0,0 %	4,1 %	12,5 %	8,7 %

Resultatene viser at trafikkdata er av betydning for flere ulike formål i sakene hvor det innhentes, men at det opplyses at det særlig brukes til *kontroll av mistenkte/siktedes bevegelser* (81,8%), *kontroll av opplysninger fremkommet i politiavhør eller andre undersøkelser* (76,8%) og til å kontrollere *opplysninger om mistenktes/siktedes kontaktmønster* (75,3%). Tallene viser også at det er variasjoner i hvilke formål trafikkdata blir benyttet til innenfor de ulike sakstypene.

3.3.4 Lagringstidens betydning

For å undersøke hvorvidt en lengre lagringstid ville medføre at ytterligere trafikkdata hadde blitt innhentet ble det stilt ytterligere et spørsmål til samtlige respondenter:

> **Hvor enig eller uenig er du i at det ville vært relevant å innhente historiske trafikkdata lengre tilbake i tid i denne aktuelle saken?**

Svarene ble inndelt i henholdsvis trafikkdata for *mobil- og fasttelefon* og for *IP-trafikk*.

Mobil-/fasttelefon

	Helt enig	Litt enig	Verken enig eller uenig	Litt uenig	Helt uenig
Samlet - alle kategorier	**50,4 %**	**9,5 %**	**15,2 %**	**3,4 %**	**21,5 %**
Drap	21,7 %	4,3 %	39,1 %	13,0 %	21,7 %
Grove narkotikasaker	56,2 %	10,0 %	15,2 %	2,5 %	16,2 %
Grove ran	44,0 %	12,0 %	12,0 %	6,0 %	26,0 %
Seksuelle overgrep	36,7 %	7,9 %	13,5 %	4,7 %	37,2 %

IP-trafikk

	Helt enig	Litt enig	Verken enig eller uenig	Litt uenig	Helt uenig
Samlet - alle kategorier	**40,8 %**	**4,0 %**	**24,3 %**	**3,5 %**	**27,5 %**
Drap	11,1 %	11,1 %	44,4 %	0,0 %	33,3 %
Grove narkotikasaker	43,3 %	4,1 %	27,1 %	2,5 %	23,0 %
Grove ran	47,6 %	4,8 %	11,9 %	7,1 %	28,6 %
Seksuelle overgrep	36,0 %	3,0 %	18,2 %	5,4 %	37,4 %

Resultatene viser at det i en stor andel av sakene, henholdsvis ca 60% for mobil-/fasttelefon og ca 45% for IP-trafikk, ville det vært aktuelt å innhente ytterligere trafikkdata dersom dette var tilgjengelig. Hva disse trafikkdataene ville bidratt til av opplysninger vet en selvsagt ikke noe om.

3.3.5 Oppsummering av resultatene fra Kripos undersøkelse

Totalt sett viser undersøkelsen at trafikkdata er en vanlig etterforskningsmetode i de undersøkte sakstypene. Trafikkdata innhentes i ca halvparten av denne typen alvorlige saker som fører til en positiv påtaleavgjørelse. I de undersøkte sakene vurderer politiet at det er viktige bevis under etterforskningen i ca 80% av tilfellene hvor trafikkdata innhentes.

I de tilfellene hvor trafikkdata ikke hentes inn i disse sakene, så skyldes dette i hovedsak at det er vurdert som et ikke nødvendig etterforskningsskritt. Saken løses med andre politimetoder enn trafikkdata. Dette viser at de ulike etterforskningsmetodene utfyller hverandre og at det er samspillet mellom metodene som er det avgjørende.

Undersøkelsen viser også at trafikkdata brukes til ulike formål i etterforskningen, men at kontroll av bevegelser, kontroll av forklaringer og analyse av kontaktmønster er opplyst som de viktigste bruksområdene for trafikkdata.

Endelig viser også undersøkelsen at det i et stort antall saker ville vært relevant å innhente ytterligere trafikkdata dersom lagringstiden var lenger.

DEL IV – Generelle kommentarer til høringsnotatet

Før vi kommenterer de spesifikke høringsspørsmålene om forslag til lagringstid, endringer i straffebud og lagringsløsning, velger vi å kommentere tre generelle problemstillinger.

4.1 Omfanget av inngrep i personvernet

Datalagringsdirektivet legger opp til lagring av trafikkdata for alle brukere av telefoni og datatjenester. Majoriteten av disse vil være lovlydige borgere. Den offentlige debatten har i stor grad dreid seg om hvilket inngrep Datalagringsdirektivet utgjør for disse. Etter Kripos oppfatning er dette et viktig hensyn, men det synes som debatten i stor grad har blitt en generell personverndebatt mer enn en debatt om det er mulig å finne en lagringsløsning som minsker inngrepet i personvernet.

Kripos mener at sikkerheten rundt lagrede data og graden av tilgjengelighet er de sentrale faktorene i denne sammenheng. Det finnes lagringsløsninger som krypterer alle data i det de genereres slik at de er komplett uleselige for alle parter, også for teletilbyderne og politiet, frem til det foreligger en rettslig kjennelse for at politiet skal ha tilgang til dataene.

Løsningen er også omhandlet i Svein Willassens utredning[25] som ble gjennomført på vegne av Datatilsynet i anledning nærværende høringsrunde.

Fra Willassens utredning siteres:

> *"(…) Risikofaktorer for personvern ved datalagring henger altså sammen med hvem dataene er eller kan være tilgjengelig for. Dette betyr at man med en vurdering av risikofaktorer for personvern ved datalagring må vurdere hvem dataene vil være tilgjengelig for. Lagring av data på en slik måte at datainnholdet ikke kan leses av noen medfører ingen risikofaktor for personvernet. (For eksempel ved kryptering med*

[25] http://datatilsynet.no/upload/Dokumenter/publikasjoner/rapporter/utredning-datatilsynet.pdf, pkt 4.5

en tilfeldig nøkkel som ikke lagres.) Motsatt vil publisering av data medføre en betydelig risikofaktor for personvernet for den dataene omhandler.

På bakgrunn av overnevnte kan den foreliggende vurderingen av risikofaktorer for personvern sies å ha en praktisk tilnærming. Dette i motsetning til en prinsipiell tilnærming der enhver lagring av data sees på som skadelig for personvernet uansett om dataene kan leses av noen eller ikke." (s 8)

Kripos er enig i dette utgangspunktet. Willassen beskriver så (pkt 4.5 i utredningen) en europeisk standard (ETSI TR 102 661) som omhandler informasjonssikkerhetstiltak som kan gjennomføres i forbindelse med kommunikasjonskontroll og datalagring, herunder en løsning for sanntidskryptering av trafikkdata. En lagringsløsning med i utgangspunktet uleselige data vil redusere misbrukspotensialet og øvrige personvernmessige betenkeligheter til et absolutt minimum.

En løsning med sanntidskryptering av data synes ikke å være utredet i forkant av høringsrunden. Kripos stiller seg undrende til dette da en slik krypteringsløsning etter Kripos syn vil minimalisert personvernmessige betenkeligheter med at data skal misbrukes, - enten ved at de brukes til andre formål enn hva de er tiltenkt eller at de skal komme på avveie.

Manglende sikringstiltak, som eksempelvis en slik krypteringsløsning, var også en av hovedinnvendingene den tyske forfatningsdomstolen hadde til implementeringen av Datalagringsdirektivet i tysk lovgivning[26].

4.2 Personvern – for hvem

I høringsnotatet[27] fremkommer det at departementene legger til grunn at direktivet er forenlig med kravene som stilles i EMK artikkel 8. Når det stilles spørsmål om direktivet er *forenlig* med artikkel 8, tas det utgangspunkt i personvernet til de som berøres av direktivet, nemlig brukerne av elektroniske kommunikasjonsmidler. En annen innfallsvinkel er å spørre om direktivet er en *forutsetning* for at Norge skal ivareta sine forpliktelser etter artikkel 8, og da med utgangspunkt i personvernet til ofrene for kriminelle handlinger. Som det fremgår av punkt 2.3.6 ovenfor, mener Kripos at direktivet er en forutsetning for at Norge skal ivareta sine forpliktelser etter FNs barnekonvensjon.

Kripos er også av den oppfatning at direktivet er nødvendig for at Norge skal verne privatlivet til den enkelte borger, slik EMK artikkel 8 foreskriver. En viser for øvrig til EMDs avgjørelse i saken K.U. mot Finland[28], som for øvrig er omtalt nærmere i Lov og Rett nr. 1-2, 2010 i artikkelen *"Datalagringsdirektivet – en menneskerettskrenkelse eller –forpliktelse"* av politiadvokat Ingvild Bruce i Økokrim[29]. I domspremissene legges det til grunn at myndighetene har en positiv forpliktelse til å sørge for mekanismer som gjør det mulig å identifisere og straffeforfølge personer som krenker andres liv, helbred og retten til privatliv. Uten en implementering av datalagringsdirektivet kan det bli vanskelig å ivareta denne forpliktelsen.

[26] http://www.bundesverfassungsgericht.de/en/press/bvg10-011en.html
[27] Høringsnotatet, pkt 1.4, andre avsnitt, s 6
[28] EMD dom av 2.desember 2008, K.U. mot Finland (saksnummer 2872/02)
[29] Lov or Rett nr 1-2 2010, s 6-26 – "Datalagringsdirektivet – en menneskerettskrenkelse eller –forpliktelse" v/Ingvild Bruce

4.3 Internasjonale forpliktelser – Norge frihavn for elektroniske spor

Norge har ved å tiltre flere konvensjoner og samarbeidsavtaler forpliktet seg til å bidra til internasjonalt politisamarbeid[30], eksempelvis gjennom Den europeiske konvensjon om gjensidig hjelp i straffesaker av 20. april 1959, Schengenkonvensjonen av 19. juni 1990 og Den nordiske politisamarbeidsavtalen av 1. januar 2003. Artikkel 1 i Den europeiske konvensjon om gjensidig hjelp i straffesaker slår fast at statene skal yte hverandre "*størst mulig gjensidig bistand*" ved forfølgning av straffbare handlinger. Sakseksemplene i dette notatets del II levner liten tvil om viktigheten og nødvendigheten av at norsk politi er rustet til å bidra til dette samarbeidet. Grenseoverskridende kriminalitet fordrer grenseoverskridende politimetoder.

Manglende evne til å bidra vil ramme våre samarbeidspartnere, men mest av alt vil det ramme oss selv. På samme måte som de kriminelle søker anonymitet i det offentlige rom vil de også søke anonymitet i cyberspace. Når et kriminelt nettverk velger sted for neste anslag vurderer de ikke bare muligheten for utbytte, men også risikoen for å bli avslørt. Dersom datalagringsdirektivet ikke innføres i Norge, frykter Kripos at organiserte kriminelle grupperinger i enda større grad vil etablere seg her, i det muligheten for å bli avslørt vil være vesentlig mindre enn i våre 23 naboland som har implementert direktivet. Og hvis Norge velger å stille seg i en situasjon hvor vi ikke er i stand til å bidra til det internasjonale politisamarbeidet, kan vi heller ikke forvente å motta hjelp tilbake. Dermed risikerer vi å bli stående alene i kampen mot den organiserte kriminaliteten.

DEL V – Lagringstid, sikringspålegg og politiets tilgang til trafikkdata

5.1 Lagringstid

Det fremgår i høringsnotatet at "*Det har blitt pekt på at politiet også med kort lagringstid har vært i stand til å oppklare store saker hvor trafikkdata utgjorde viktige bevis, så som Baneheia-saken og Nokas-saken*"[31]. Kripos er enig i den påfølgende drøftelsen i høringsnotatet hvor det fremkommer at det er *"…lite ønskelig at avsløringen av store straffesaker skal bero på tilfeldige avvik i lagringsperioden mellom tilbyderne."*

At trafikkdata i fremtiden vil ha mindre betydning for teletilbyderne er hovedbegrunnelsen for at det må skapes en forutsigbarhet i hvilke spor som skal lagres for etterforskningsformål.

Lagringspraksis har de senere år variert basert på de ulike teletilbydernes behov for fakturering. Fra 6 måneders lagring til dagens praksis med 3-5 måneders lagring. Eksempelvis ville viktige data som ble innhentet i Orderud-saken i 1999 ut fra lagringspraksisen den gang vært tapt dersom dagens lagringspraksis hadde vært gjeldende. Det er betenkelig at slike tilfeldige forhold skal avgjøre hvilke trafikkdata som er tilgjengelige for etterforskningsformål.

[30] Se også NOU 2009:15, pkt 8.3, s 69
[31] Høringsnotatet, pkt 48, s 41

5.1.1 Begrunnelse for minst 1 års lagringstid

Majoriteten av landene som har innført Datalagringsdirektivet har valgt 1 års lagringstid.

Dersom en skulle hensynta alle tenkelige etterforskningsmessige behov, burde ideelt sett trafikkdata aldri bli slettet, men være mulig å fremskaffe uansett når behovet måtte oppstå. Gjennom langvarige etterforskninger og et økende antall gjenopptagelsessaker vil det være et reelt behov også utover 1 års lagring av trafikkdata. Departementene beskriver også et behov utover 1 års lagringstid i høringsnotatet[32]. Kripos støtter disse vurderingene.

Kripos er imidlertid enig i at det må foretas en avveining opp mot personvernet og hensiktsmessigheten av å lagre data i lang tid. For de fleste sakstyper innen Kripos' ansvarsområde vil det kunne være behov for en lagringstid på 1 år. I noen saker vil også dette være for lite, men i lys av avveiningen som må foretas opp mot personvernet, og sett hen til implementeringen i våre naboland, mener Kripos at 1 års lagringstid er tilstrekkelig for saker innenfor vårt saklige ansvarsområde. Andre politienheter kan imidlertid ha behov for lengre lagringstid, ut fra sine saklige ansvarsområder[33].

Kripos sitt behov for 1 års lagringstid begrunnes med følgende:

5.1.1.1 I hovedsak reaktiv etterforskning

I all hovedsak er politiets etterforskning reaktiv. Etterforskningen starter ved at politiet får melding om en hendelse som allerede har funnet sted. Etterforskningens formål er å avdekke hva som har skjedd og hvem som skal stilles til ansvar for handlingen. Politiet må forsøke å gjenskape et hendelsesforløp. For å få til dette må man derfor gå bakover i tid for å finne relevante opplysninger. Trafikkdata er meget godt egnet til dette da telefon/datamaskin brukes langt hyppigere enn eksempelvis et kredittkort, bombrikke eller andre elektroniske spor som kunne vært relevante å innhente.

Hvor langt tilbake i tid man må gå avhenger av en rekke faktorer, blant annet hvor lang tid det går fra gjerningstidspunktet til politiet får melding om hendelsen, hvor mange forberedelseshandlinger som er relevante å undersøke, omfanget av saken osv.

I en del saker vil ikke politiet få kjennskap til det straffbare forholdet før lenge etter at det fant sted eller at etterforskningen dreier seg om straffbare forhold som har skjedd over en lang tidsperiode. Det vises til saksgjennomgangen i pkt 2.3.

5.1.1.2 Etterforskning er en dynamisk prosess

Det er viktig å forstå at etterforskning er en dynamisk prosess. Man vet ikke hvilken informasjon som er relevant ved etterforskningens begynnelse. Av denne grunn vet man heller ikke i starten av saken hvilke trafikkdata man har behov for, og dermed kan heller ikke de relevante trafikkdata fryses gjennom sikringspålegg etter strpl §215a. Informasjon som innhentes gjennom avhør, tekniske undersøkelser, ransaking/beslag, analyse av trafikkdata mv. medfører behov for ytterligere trafikkdata.

Etterforskning kan beskrives som et puslespill hvor man i starten ikke vet hvordan det fullstendige bevisbildet skal se ut, og dermed ikke hvilke biter man har behov for. Når det

[32] Høringsnotatet pkt 4.8, s 40
[33] Se også innledningen til Del II, tredje avsnitt

gjelder trafikkdata kan de relevante bitene være borte på grunn av kort lagringstid når behovet oppstår. Dermed blir ikke bevisbildet fullstendig.

Det vises til saksgjennomgangen i pkt 2.3, særlig til beskrivelsen av saknetsaker, drapssaker og sedelighetssaker.

5.1.1.3 Økt grad av profesjonalisering
Gjennomføring av alvorlig kriminalitet har blitt mer profesjonalisert, særlig den grove og organiserte kriminaliteten. Det betyr at de mistenkte i større grad nå enn tidligere tar i bruk motstrategier for å unndra seg politiets etterforskning, se også pkt 1.2. Det vises til at det er vanlig at de mistenkte hyppig skifter telefonnummer og telefonapparater fordi de vet at politiet undersøker denne type spor, de bruker internetcafe'er, falske dokumenter og krypterte kommunikasjonstjenester mv.

Dette medfører *ikke* at de straffbare forholdene er umulig å avdekke og etterforske for politiet, men etterforskningen vil i disse tilfellene ta vesentlig lenger tid. Kartlegging av hvilke motstrategier som er benyttet og hvor man skal finne alle spor er tidkrevende. Jo lenger lagringstiden for trafikkdata er, dess vanskeligere blir det å gjennomføre mottiltak fra de mistenkte. Departementene har også beskrevet dette i høringsnotatet[34]. Kripos støtter vurderingene til departementene på dette punktet.

Dette er et forhold som med tyngde taler for at lagringstiden må være så lang at politiet til tross for disse motstrategiene har mulighet til å sikre relevante spor, blant annet all relevant trafikkdata.

5.1.1.4 Økende grad av internasjonal etterforskning
Den økende graden av internasjonal etterforskning har også stor betydning. De kriminelle er i større grad mobile og opererer over landegrensene. Samtidig har politiet i større grad fokusert på bakmenn for organisert kriminalitet. Begge disse forholdene resulterer i at det mer enn tidligere må innhentes informasjon i utlandet gjennom internasjonalt politiarbeid.

Resultatet av undersøkelsene i utlandet kan foranledige behov for ytterligere trafikkdata i Norge eller i utlandet. Forsinkelsen som følge av det internasjonale samarbeidet gjør at trafikkdata kan gå tapt på grunn av kort lagringstid.

5.1.1.5 Økende grad av fokus på bakmenn
Politiets etterforskning har de senere årene rettet seg mer inn mot bakmenn for alvorlig kriminalitet. Det vises blant annet til beskrivelsen under pkt 2.3.3 – Narkotikasaker.

Politiets fokus er i hovedsak mot de konkrete straffbare forhold, og dersom man skal kartlegge og ramme de organisatoriske elementene må man som oftest gå flere ledd ut i kjeden. Kommunikasjon mellom bakmenn og deres strømenn som utfører de risikofylte oppgavene skjer ofte på egne telefonnummer slik at risikoen for å bli oppdaget skal være minst mulig. For politiet er det utfordrende og tidkrevende å avdekke disse nettverkene av hemmelige/anonyme telefoner mellom bakmenn og deres strømenn, og trafikkdata er således meget viktige bevis. Ofte avdekkes ikke de aktuelle numrene før politiet gjennomfører ransaking og beslag i forbindelse med pågripelsesaksjoner. Trafikkdata kan da være tapt.

[34] Høringsnotatet, pkt 4.8, s 41

5.1.1.6 Mistenkte har rett til ikke å bidra til opplysning av saken
Et annet forhold er at mistenkte har en lovbestemt rett til ikke å avgi forklaring. Etterforskningen av alvorlige saker kan ta flere år. Erfaringsmessig benytter mange seg av retten til å ikke avgi forklaring, i alle fall innledningsvis. Dersom mistenkte velger å forklare seg på et senere tidspunkt, kan viktige trafikkdata som kan bekrefte/avkrefte mistenktes forklaring være tapt.

Det er vanlig at det sent i saken fremkommer forklaringer om alternative gjerningsmenn eller andre impliserte, eller om rollefordeling og andre spørsmål av betydning for straffutmålingen. Trafikkdata er ofte den beste muligheten til å ettergå slike forklaringer. Dette gjelder både opplysninger som kan tale til mistenktes gunst og ugunst.

Når forklaringene kommer sent, kan nøyaktigheten i vitneforklaringer være dårligere, særlig rundt detaljer som å fastsette tidspunkter for ulike hendelser. I denne sammenheng er trafikkdata ofte det eneste objektivt kontrollerbare bevis som kan bekrefte eller avkrefte en forklaring. Dersom trafikkdata ikke kan fremskaffes på grunn av kort lagringstid, noe som ofte er en relevant problemstilling med dagens lagringspraksis, så vet også de mistenkte at forklaringene i liten grad kan ettergås. Dette medfører en usikkerhet rundt forklaringenes troverdighet. Forklaringene kan bli stående som ukontrollerbare påstander.

5.1.1.7 Mistenktes mulighet til å imøtegå anklager
Forklaringer som kommer sent i saken har ikke bare relevans for mistenkte, men kan også ha betydning for andre mistenkte i samme sak. Det er av denne grunn viktig at politiet har mulighet til å ettergå forklaringene for å undersøke om det er hold i opplysningene.

Et moment i denne forbindelse er bruk av klausulering av dokumenter i forbindelse med etterforskningen, jfr strpl §242. Klausulering innbærer at en rekke opplysninger av polititaktiske årsaker unntas fra siktedes innsyn innledningsvis i etterforskningen. I disse tilfellene er det vanskelig for siktede å ha oversikt over hvilke opplysninger som ligger til grunn for anklagene mot ham/henne.. Av denne grunn er det også vanskelig for siktede å vite hvilke trafikkdata som eventuelt kunne ha vært egnet for å imøtegå anklagene mot ham/henne.

Til tross for at det er påtalemyndigheten som har bevisbyrden i straffesaker, har siktede rett til – og ofte et ønske om – å imøtegå anklagene og be om at politiet utfører visse etterforskningsskritt, jfr bl.a. strpl. § 92. Trafikkdata er et bevis som normalt er godt egnet til å bekrefte eller avkrefte opplysninger som fremkommer i saken.

Straffeloven § 172 oppstiller en opplysningsplikt for å forebygge at en uskyldig (som er tiltalt) blir dømt eller at straffen overfor en uskyldig blir fullbyrdet. Trafikkdata er også et egnet hjelpemiddel til å sjekke personer ut av saken på et tidligere stadium. For en uskyldig som har vært i politiets søkelys - eksempelvis etter tips fra publikum - og fått status som mistenkt, vil det normalt være ønskelig å få saken så godt opplyst at den kan henlegges som "intet straffbart forhold bevist", og ikke på "bevisets stilling". Dette vil naturlig nok også være i politiets interesse. Trafikkdata kan i den forbindelse nyttes for å etterprøve og underbygge mistenktes og andres forklaringer.

5.1.1.8 Domstolenes behov for å få saken belyst

Politiets etterforskning danner grunnlaget for bevistilbudet retten blir gitt under hovedforhandling. Domstolenes behov for å få saken tilstrekkelig opplyst før det avsies dom følger av strpl §294. Domstolens mulighet til å innhente nye bevis - eller kontrollere holdbarheten av bevis som fremlegges - er imidlertid helt avhengig av hvilken informasjon som kan fremskaffes.

Det varierer mye hvor lang tid det går fra tidspunktet for det straffbare forhold til saken behandles av domstolen, men det er vanlig at det tar mer enn 6 måneder, tidvis også lenger enn 1 år. Erfaringsmessig fremkommer det ofte nye opplysninger under hovedforhandlingen.

Hvorvidt domstolen kan legge til grunn de nye opplysningene som fremkommer under hovedforhandling, avhenger av muligheten for å kontrollere troverdigheten av opplysningene. Lagringstiden for trafikkdata bør også hensynta dette behovet.

Et annet moment er at siktedes grad av skyld vektlegges i norsk strafferett. Til tross for at domstolen kun kan domfelle når det foreligger bevis for skyld "*utover en hver rimelig tvil*" så vil også sakens opplysning avgjøre hvilke roller de ulike tiltalte blir tillagt. Dette har betydning for staffeutmålingen. Eksempelvis straffes en narkotikakurer langt mildere enn den som har organisert innførselen. Domstolen har behov for at saken er godt opplyst, også om forhold som går utover spørsmålet om skyld.

5.1.2 Skille på lagringstid for ulike teknologier

Kripos er enig i departementenes vurdering av at det ikke bør skilles i lagringstid for ulike teknologier. Det er viktig at lovgivningen er teknologinøytral slik at den også fanger opp den teknologiske utviklingen. Det bør være uinteressant hva som er databæreren for kommunikasjonen som foretas mellom to eller flere personer, dvs. at datatypen som lagres er uavhengig av om dataene er bragt frem ved bruk av IP-baserte tjenester eller vanlig telefoni. Forkjeller i lagringstid basert på teknologi vil medføre at de mistenkte tilpasser seg dette da de tar forholdsregler mot politiets etterforskning. Kripos mener derfor at lagringstiden for både IP-basert kommunikasjon og vanlig teletrafikk bør være lik og at den settes til minst 1 år. Teleplans undersøkelser viser også at lagringstiden i liten grad påvirker kostnadene for lagring[35].

5.1.3 Vil en økt lagringstid ha en "nedkjølende effekt"?

Høringsnotatet beskriver som et moment mot lenger lagringstid enn 6 måneder at dette kan ha en "*nedkjølende effekt*" på borgernes vilje til åpen og fri kommunikasjon. Kripos stiller seg tvilende at direktivet vil ha en slik effekt, og dersom et slikt hensyn skal hensyntas så må dette være basert på at det faktisk kan påvises en slik klar effekt og årsakssammenheng i evalueringen av implementeringen av direktivet i de øvrige europeiske land som skal sluttføres innen 15. september 2010.

[35] Høringsnotatet, s 53

5.2 Sikringspålegg – strpl §215a

Høringsnotatet omtaler påtalemyndighetens mulighet til å gi sikringspålegg etter strpl. §215a[36]. Dette har sin relevans i de tilfellene hvor politiet vet hvilke data som skal sikres, men at dataene vil kunne gå tapt før påtalemyndigheten har rukket å innhente dem.

Sikringspålegg er sjelden aktuelt slik praksis er i dag. Behandlingstiden hos Post- og Teletilsynet og retten overstiger sjelden to dager, og da er sikringspålegg kun aktuelt hvor data som ønskes sikret er i ferd med å bli slettet, dvs. data som er nøyaktig 3 måneder, 5 måneder eller 21 dager gamle (den maksimale lagringstiden), alt avhengig av hvem som besitter dataene.

Dersom politiet vet at noen tilbydere (ISP'er) sletter data før den tillatte lagringstiden, kan bruken av sikringspålegg være aktuelt. Et annet tilfelle er hvor politiet mottar rettsanmodinger fra utlandet og hvor de formelle reglene rundt oversendelsen er tidkrevende. Politiet vil i disse tilfellene kunne utstede et sikringspålegg for teletilbyderne i påvente av at den offisielle begjæringen fra utlandet oversendes.

Bruk av sikringspålegg var likevel mest aktuelt for noen år siden hvor teletilbydernes behandlingstid var meget lang. Det kunne ta flere måneder fra anmodningen om trafikkdata ble sendt teletilbyderen til data faktisk ble utlevert. Da ville denne typen sikringspålegg sørge for at teletilbyderne sikret data før de gikk tapt. Dette har endret seg vesentlig, og teletilbyderne leverer nå data normalt sett i løpet av noen få dager.

Kripos har rettet forespørsel til Telenor og Netcom som opplyser at de mottar sikringspålegg fra påtalemyndigheten ca 10-20 ganger hvert år. Kripos mener derfor at anførselen fra Post- og Teletilsynet i høringsnotatet[37] om at politiet "*i noen grad*" bruker bestemmelsen er noe unøyaktig.

Det er av flere blitt hevdet at sikringspålegg etter strpl §215a reduserer behovet for lagring av trafikkdata. Dette er Kripos uenig i. For det første krever sikringspålegg at det faktisk er data å sikre, hvilket forutsetter at data lagres. For det andre er det en forutsetning at en vet hvilke data en har behov for. Som beskrevet under pkt 5.1 ovenfor, er det nettopp dette som er utfordringen for politiet i starten av en etterforskning.

Etter hvert som politiet får kunnskap om hvilke data som er relevante å innhente, innhentes disse snarest mulig. Det er da lite å tjene på et sikringspålegg siden den formelle prosessen tar kort tid og fordi teletilbyderne har kort behandlingstid.

Sikringspålegg bør fortsatt være tilgjengelig for påtalemyndigheten, men det løser ikke problemet med kort lagringstid.

5.3 Politiets tilgang til trafikkdata

Forutsatt at direktivet innføres må det også tas stilling til på hvilke vilkår politiet skal gis tilgang til de data teletilbyderne lagrer. I den forbindelse er det ikke bare relevant å se hen til formålet med direktivet og hvordan dette er implementert i andre lands lovgivning, men også hvordan en innføring på de foreslåtte vilkår vil harmonere eller disharmonere med eksisterende straffeprosessuelle bestemmelser i norsk rett. Selv om direktivet ble vedtatt for

[36] Høringsnotatet, pkt 2.4.1, s 12-13
[37] Høringsnotatet, pkt 2.5, s 19

å bekjempe "*alvorlig*" kriminalitet og innebærer at trafikkdata skal lagres av andre hensyn enn tidligere, må det tas i betraktning at bruk av trafikkdata i etterforskningsøyemed har eksistert i lang tid, og at de strenge vilkårene som er foreslått for implementering av direktivet vil innebære en markant endring i forhold til dagens rettstilstand.

5.3.1 Dagens rettstilstand[38]

Etter gjeldende rett kan historiske trafikkdata innhentes på følgende hjemmelsgrunnlag:

1. Straffeprosessloven §203 (beslag)
2. Straffeprosessloven §210 (utleveringspålegg)
3. Straffeprosessloven §216 b annet ledd bokstav d (kontroll av kommunikasjonsanlegg)
4. Straffeloven §47 (nødrett)
5. Samtykke fra abonnenten

Som nevnt i NOU 2009:15 s 218 første spalte, er det i praksis beslagsbestemmelsen som i dag brukes av politiet ved innhenting av trafikkdata.[39] Siden teletilbyderne har taushetsplikt etter ekomloven §2-9, må politiet først skrive en anmodning til (PT) om fritak fra taushetsplikten, hvor det redegjøres for bevisets betydning for etterforskningen. Selv om det etter §203 ikke gjelder noe strafferammekrav, oppgir politiet hvilket forhold som er under etterforskning. Dette fordi all bruk av tvangsmidler fordrer en konkret forholdsmessighetsvurdering, jfr strpl §170a.

Dessuten gir strpl §118 anvisning på en konkret avveining mellom hensynet til taushetsplikten og hensynet til sakens opplysning, og dette må PT vurdere før de fatter sin beslutning. Dersom PT finner at vilkårene for å frita fra taushetsplikten er til stede, formuleres en skriftlig beslutning som returneres politiet. Påtalemyndigheten skriver deretter en beslutning om beslag, hvor det henvises til PTs fritak, som også vedlegges beslutningen. Dersom PT finner at vilkårene for å frita fra taushetsplikten ikke er tilstede, kan påtalemyndigheten bringe spørsmålet inn for retten, som har kompetanse til å overprøve dette, jfr strpl §118 annet ledd.[40]

§216 b annet ledd bokstav d, gir hjemmel for innhenting av både historiske og framtidige trafikkdata. Bestemmelsen er en del av lovens kapittel 16a om kommunikasjonskontroll. og er anvendelig i mange av de saker som ligger under Kripos ansvarsområde. Dersom datalagringsdirektivet ikke innføres, og teleleverandørene ikke lenger lagrer sine data, vil bestemmelsen i framtiden bare være praktisk anvendelig for framtidige trafikkdata. Den vil følgelig få et snevrere anvendelsesområde enn lovgiver forutsatte da bestemmelsen ble vedtatt.

---

[38] Gjeldende rett og praksis er omtalt i NOU 2009:15 punkt 20.2. Verken strpl §203 eller §210 oppstiller noe strafferammekrav.

[39] I tilfeller hvor det er behov for utsatt underretning brukes i praksis utleveringspålegg. Dette fordi det er retten som har kompetanse til å beslutte utsatt underretning, både om beslag og utleveringspålegg, jf. hhv. §208a og §210a. Da er det mest hensiktsmessig at retten samtidig tar stilling til om beviset skal utleveres. Teletilbyderne er omfattet av strpl§118, slik at Post- og teletilsynet (PT) må frita fra taushetsplikten etter ekomloven §2-9 før retten kan pålegge utlevering. Se bl.a. RG 2008 s 1477

[40] I en sak Kripos etterforsket våren 2008 ble det beslaglagt ca 150 kg hasj i en nederlandsk trailer. Kureren forklarte at han hadde mottatt hasjen i Norge fra en annen sjåfør. I tiden rundt overleveringen hadde han hatt jevnlig kontakt med en koordinator i Nederland. Koordinatorens telefon hadde i samme tidsrom vært i hyppig kontakt med et annet nederlandsk nummer, og Kripos anså trafikkdata fra dette nummeret for å ha betydning som bevis i saken, uten at vi på det tidspunktet hadde grunnlag for en konkret mistanke mot brukeren. PT fritok ikke teletilbyder fra taushetsplikten. Oslo tingrett overprøvde dette, og trafikkdata ble innhentet. Dataene viste at nummeret hadde befunnet seg i nøyaktig samme område i Norge som den pågrepne kureren på tidspunktet for overleveringen. På dette grunnlag ble brukeren – som hadde fraktet hasjen fra Nederland til Norge - identifisert, pågrepet og besluttet utlevert fra Nederland til Norge for straffeforfølgning her. Uten trafikkdata ville oppklaringen av saken ikke vært mulig. Saken er ikke rettskraftig.

5.3.2 Foreslåtte vilkår

- Krav om 3 års strafferamme
- Krav om skjellig grunn til mistanke mot en bestemt person
- Krav om rettslig prøving (utleveringspålegg)

I det følgende vil en kommentere disse forslagene nærmere.

5.3.2.1 Kravet om 3 års strafferamme

Det siste tiåret har politi og påtalemyndighet fått nye verktøy, som er tilpasset utviklingen i det samfunnet vi er satt til å beskytte. Trafikkdata har lenge vært et av basisverktøyene, som vi har kunnet benytte til å løse de fleste pålagte oppgaver. Dersom implementeringen av direktivet i norsk rett gjøres på de foreslåtte vilkår, innebærer det at basisverktøyet heretter bare kan benyttes til å løse de mest alvorlige oppgavene, til tross for at det fortsatt er like effektivt i andre tilfeller. I tillegg til å være et effektivt verktøy er det som regel også forholdsmessig å bruke det. Et viktig prinsipp i etterforskningen er som kjent forholdsmessighetsprinsippet; inngrepets art må stå i forhold til sakens alvor og omfang.

Det er relevant å sammenligne forslaget til ny §210 første ledd med vilkårene for å bruke andre tradisjonelle metoder. Vilkårene for ransaking etter §195 er at "*noen med skjellig grunn kan mistenkes for en handling som etter loven kan medføre frihetsstraff*". Den primære beslutningskompetansen tilligger retten, men påtalemyndigheten har sekundærkompetanse. Dette betyr i praksis at politiet, i en rekke tilfeller hvor den foreslåtte strafferammen for innhenting av trafikkdata ikke er til stede, har anledning til å ransake mistenktes bopel, beslaglegge mobiltelefonen og sikre innholdet. Dette framstår som et større inngrep enn det å innhente historiske trafikkdata. Et grunnleggende prinsipp for politiets etterforskning er subsidiaritetsprinsippet; det minst inngripende virkemidlet må være forsøkt først. Å oppsette strengere vilkår for innhenting av trafikkdata enn det som gjelder for antatt mer inngripende tvangsmidler vil bryte med dette prinsippet. Eksemplet illustrerer at departementets forslag om 3 års strafferamme harmoniserer dårlig med vilkårene for bruk av andre tvangsmidler i norsk rett.

Strpl§215a, hvoretter påtalemyndigheten kan gi sikringspålegg, har samme inngangsvilkår som §§203 og 210, nemlig at dataene "*antas å ha betydning som bevis*" i etterforskningen. I Ot.prp.nr. 40 (2004-2005) fastslås at bestemmelsen omfatter trafikkdata. Dersom §210 endres som foreslått i høringsnotatet, uten at det samtidig gjøres en endring i §215a, vil det medføre at påtalemyndigheten har en langt videre adgang til å gi sikringspålegg enn det domstolene vil ha til å pålegge utlevering av de samme dataene. Dette illustrerer at vilkårene som foreslås i høringsnotatet vil gi et inkonsekvent nasjonalt regelverk.

Kravet om 3 års strafferamme vil neppe få særlig betydning for muligheten for å oppklare saker som ligger under Kripos saklige kompetanseområde, siden disse sakstypene normalt har høyere strafferamme. Noen unntak vil det likevel være, blant annet i tilfeller hvor vi yter bistand[41] eller deltar i felles etterforskningsgrupper. For politidistriktene, som har ansvar for etterforskning av alle sakstyper innenfor sitt geografiske område, vil strafferammekravet få større betydning.

---

[41] Fra NOU 2009:1 – "Personvern i det digitale samfunnet", pkt. 14.3.4: "*På et populært nettsted i Norge har det blitt laget en falsk profil over en 13 år gammel jente hvor det opplyses at hun ønsker sex med voksne menn og fantaserer om å bli voldtatt hjemme. Profilen inneholdt korrekte og utfyllende personopplysninger. Saken ble politianmeldt og det viste seg at profilen var opprettet av en person i jentas omgangskrets og resultat av en uenighet*". Mulig brudd på strl. §390a. Strafferamme: 2 år. Saken ville ikke blitt oppklart med dagens lagringspraksis. Det gikk mer enn 21 dager fra profilen var opprettet på nettstedet (og IP adressen til brukeren ble lagret) til politiet kunne kontakte vedkommende ISP. På det aktuelle tidspunktet var lagringstiden 3-5 måneder, og abonnenten kunne da identifiseres.

Problemet med den valgte lovgivningsteknikken - et høyt strafferammekrav kombinert med enkelte positivt angitte straffebud – er at det er særdeles vanskelig å ha en begrunnet oppfatning av hvilke straffebud som skal omfattes. Dette fordi trafikkdata er en type bevis som har betydning i nær sagt alle sakstyper. Som eksempel nevnes straffeloven §201. Av annet ledd fremgår eksplisitt at bestemmelsen rammer handlinger forøvet gjennom bruk av telefon, internett eller annen elektronisk kommunikasjon. Muligheten til å oppklare slike forhold dersom bestemmelsen ikke lenger gir grunnlag for å innhente trafikkdata vil bli illusorisk. Det er umiddelbart vanskelig å se hvorfor en skal kunne innhente trafikkdata i § 201a-saker, men ikke i §201-saker.

Den valgte lovgivningsteknikken fordrer en langt grundigere gjennomgang av samtlige straffebud enn den høringsnotatet gir uttrykk for. Også spesiallovene må i så fall gjennomgås og vurderes inntatt, eksempelvis forurensningsloven §78[42]. I tillegg må en se hen til straffeloven av 2005, som formentlig trer i kraft i løpet av de nærmeste årene. Kapittel 21 omfatter straffebud som etter sin art fordrer innhenting av trafikkdata i etterforskningen. Strafferammen er hovedsaklig 2 år[43]. Det er grunn til å stille spørsmål ved om politiet vil være i stand til å håndheve de nye reglene dersom forslaget i høringsnotatet vedtas.

5.3.2.2 Kravet om skjellig grunn til mistanke mot en bestemt person

Forslaget om at det må foreligge skjellig grunn til mistanke mot en bestemt person for å innhente trafikkdata skiller seg markant fra dagens regelverk. Etter dagens §210 gjelder som kjent ikke noe slikt krav.

De senere årene har det vært flere tilfeller av trusler mot skoler. I en innledende fase av etterforskningen kan mistanken rette seg mot flere personer, uten at det foreligger skjellig grunn til mistanke mot noen av disse. Dersom forslaget vedtas vil det redusere muligheten til å identifisere gjerningspersoner i disse sakene. Siden dette ofte er mindreårige som trenger samfunnets hjelp, og som utgjør en potensielt stor trussel mot både eget og andres liv, er det uheldig dersom politiet mister muligheten til å benytte trafikkdata til å fange dem opp.

Videre er det relevant å sammenligne forslaget til ny §210 med vilkårene for utvidet ransaking, jfr strpl. kapittel 15. §192 tredje ledd hjemler såkalt 3. mannsransaking, hvoretter det må foreligge skjellig grunn til mistanke om en straffbar handling. Det er imidlertid ikke krav om at mistanken er rettet mot en bestemt person. Videre kan politiet i etterforskningsøyemed, med hjemmel i §193, foreta ransaking av alle steder som etter sin art er tilgjengelig for alle. På samme måte kan politiet ransake militære bygninger og rom. At vilkårene for å innhente trafikkdata skal være andre – og presumtivt strengere – enn vilkårene for å ransake – gir en ubalanse i lovverket.

Forslaget rammer også politiets mulighet til å etterforske andre forhold enn de som umiddelbart framstår som straffbare. Straffeprosessloven §224 fastslår at "*etterforskning foretas når det som følge av anmeldelse eller andre omstendigheter er rimelig grunn til å undersøke om det foreligger straffbart forhold som forfølges av det offentlige*", og med hjemmel i siste ledd "*kan*" det ved brann

[42] *Full City-ulykken (2009).* En større oljetanker gikk på grunn utenfor Langesund juli 2009. Store naturområder i ytre Oslofjord ble rammet av forurensing av olje fra havaristen. Spørsmålet var hvorvidt kapteinen på havaristen "Full City" hadde varslet om den potensielle faren når skipet mistet motorkraft og begynte å drive. Etterforskningen har stor betydning for å klarlegge både hendelsesforløpet og ansvarsforhold. Trafikkdata vil i denne type tilfeller være eneste mulighet til å undersøke hvem som ble varslet på hvilket tidspunkt.

[43] Se eksempelvis ny §202 om identitetstyveri som har en strafferamme på 2 år. Dette illustrerer for øvrig at det ikke nødvendigvis er en motsetning mellom personvern og lagring av trafikkdata. Spørsmålet er hvem sitt personvern man skal beskytte.

og andre ulykker foretas etterforskning om årsaken "*selv om det ikke er grunn til mistanke om et straffbart forhold*". Å etterforske slike saker utgjør en vesentlig del av politiets oppgaver, og trafikkdata brukes regelmessig i etterforskningen[44]. Se også pkt 2.3.9.

De eksisterende straffeprosessuelle hjemler dekker de aller fleste tilfeller hvor det er aktuelt å innhente trafikkdata. I tilfeller hvor nødrett påberopes som grunnlag er dette normalt på grunn av tidsaspektet, og ikke fordi vilkårene for å innhente trafikkdata ikke er til stede. Dersom datalagringsdirektivet innføres på de foreslåtte vilkår vil det stille seg annerledes.

Saknetsakene[45] er et godt eksempel på dette. Når pårørende melder en person saknet, har politiet en plikt til å undersøke forholdet. Innhenting av trafikkdata vil være et relevant etterforskningsskritt. I et slikt tilfelle kan riktignok nødrettsbestemmelsen i strl §47 anvendes, men det er neppe noen god løsning fra lovgivers side å overlate alle slike vurderinger til utøvende myndigheter. Inngrepets art tilsier en klar lovhjemmel, blant annet av hensyn til forutberegneligheten.[46] Nødrettsbestemmelsen er ment å være en snever sikkerhetsventil som kun kommer til anvendelse dersom handlingen ikke har (annen) hjemmel i lov.

På denne bakgrunn anbefaler Kripos at det ikke oppstilles noe vilkår om at det må foreligge skjellig grunn til mistanke mot en bestemt person. Subsidiært må det i så fall lovfestes et unntak for etterforskning hjemlet i strpl §224 fjerde ledd, samt saknetsaker og redningsaksjoner.

Videre må bestemmelsen formuleres slik at også stedsspesifikke spor[47] kan innhentes uavhengig av om noen bestemt person kan mistenkes for handlingen[48].

5.3.2.3 Hvem skal ha kompetanse til å beslutte innhenting?

Innhenting av trafikkdata er etter dagens regelverk underlagt minimum en dobbelt kontroll, bortsett fra ved nødrett og samtykke.[49] Kripos erfaring er at PT besvarer anmodningene raskt, og at dette ikke er noe forsinkende ledd. PT mottar årlig omlag 1800-1900 anmodninger om samtykke til opphevelse av taushetsplikten[50]. Dersom retten i framtiden skal behandle alle disse anmodningene må en ta høyde for både merbelastningen og kostnadene. I NOU 2009:15 kapittel 20 foreslås at innhenting av trafikkdata kun kan skje ved rettslig utleveringspålegg. Det foreslås også å endre ekomloven §2-9 slik at det ikke er nødvendig at PT opphever taushetsplikten i forkant.

En regel om at innhenting av trafikkdata bare kan skje ved rettslig utleveringspålegg vil bryte med straffeprosesslovens nåværende system. Som nevnt har påtalemyndigheten primærkompetansen til å beslutte beslag, uansett hvilken "*ting*" det er snakk om, men spørsmålet om beslaget skal opprettholdes kan kreves brakt inn for retten, jfr strpl §208. Påtalemyndigheten kan følgelig beslutte beslag i dagbøker, fotoalbum, brev, filmer og andre personlige eiendeler. Det er heller ikke noe absolutt krav om at beslaget må begrenses til mistenktes eiendeler. Det avgjørende er om det "antas å ha betydning som bevis".

---

[44] Se punkt 2.3.9.
[45] Se punkt 2.3.2
[46] Dette er for øvrig vurdert i Ot.prp.nr.59 (2003-2004), som det vises til under punkt 6.1 nedenfor
[47] Se pkt 2.1 og 2.3
[48] Se kommentarer til lovforslaget i pkt 6.1
[49] Ved bruk av hastekompetansen i §210 annet ledd er kontrollen tredobbel, både PT, politiet og retten vurderer saken.
[50] NOU 2009:15 – "Skjult informasjon – åpen kontroll", s 126 og pkt 3.1 i dette høringssvar

Kripos mener på denne bakgrunn at inngrepets art ikke kan brukes som begrunnelse for at innhenting av trafikkdata ikke kan besluttes av påtalemyndigheten. Derimot ser en at det er uheldig at framgangsmåten for innhenting varierer så vidt mye, og at den blant annet beror på hvilke krav de ulike tilbyderne stiller. Krav om rettslig utleveringspålegg vil i alle fall sikre en ensartet praksis, noe Kripos anser som en fordel.

Det er imidlertid vanskelig å forstå hvorfor retten ikke bare skal ha en primær beslutningskompetanse, men at kompetansen også skal være eksklusiv. Norsk straffeprosess bygger på et system hvor etterforskningen, herunder bruk av tvangsmidler, i stor grad er underlagt påtalemessig kontroll[51] Dette til forskjell fra flere av EU-landene hvor etterforskningen er dommerstyrt. Straffeprosesslovens system er oppbygd slik at der hvor retten har primærkompetansen til å beslutte tvangsmidler, har påtalemyndigheten en sekundær kompetanse.

Dette gjelder også for de tvangsmidler som regnes som aller mest inngripende; kommunikasjonskontroll og romavlytting, jfr strpl §216d, hvor politimesteren er tillagt "hastekompetanse"[52]. Denne hastekompetansen er i mange tilfeller helt nødvendig for at politiet skal rekke å sikre bevisene. Siden trafikkdata er en type bevis som normalt genererer ytterligere etterforskningskritt, er det viktig å få innhentet disse raskt. Eksempelvis kan trafikkdata avdekke gjerningspersonen og gi grunnlag for en snarlig pågripelse, som igjen forhindrer gjentakelse, unndragelse og/eller bevisforspillelse.

Dersom retten skal ha en eksklusiv kompetanse til å beslutte dette må det innføres en vaktordning ved domstolene, slik at det er mulig å få behandlet spørsmålet utenfor vanlig arbeidstid. Hvis politiet får melding om et drap med ukjent gjerningsmann fredag kveld er det ikke forsvarlig å avvente med sentrale deler av etterforskningen til retten åpner mandag. I et tilfelle hvor ingen vitner til handlingen melder seg vil trafikkdata være avgjørende for å oppklare saken, og initialfasen er særdeles viktig.

De økonomiske og administrative konsekvensene av å legge en eksklusiv beslutningskompetanse til domstolen synes ikke å være nærmere utredet av departementene. Kripos har ikke grunnlag for å mene noe sikkert om konsekvensene, men antar at alternativet til hastekompetanse er en form for vaktordning ved domstolene som formodentlig både vil bli kostnadskrevende å reise en del prinsipielle og praktiske spørsmål i forhold til domstolsorganiseringen. Det synes lite gjennomtenkt dersom dette skal gjelde kun for trafikkdata, når politiet vitterlig har hastekompetanse ved bruk av øvrige, til dels mer inngripende tvangsmidler.

Kripos vil på denne bakgrunn sterkt fraråde å gjøre unntak fra strpl §210 annet ledd om hastekompetanse for trafikkdata.

DEL VI - Kommentarer til de enkelte straffebudene

Kripos vil i det følgende kommentere enkelte av lovforslagene i høringsnotatets punkt 8 nærmere, på bakgrunn av våre forutgående innspill og vurderinger.

[51] Se NOU 2009:15 punkt 11.8. hvor dette beskrives nærmere.
[52] Se også NOU 2009:15 - "Skjult informasjon – åpen kontroll", pkt 15.3, s 166

6.1 Kommentarer til straffeprosessloven ny §210

Hvis en ser forslaget til nytt første ledd i §210 i sammenheng med resten av den nåværende bestemmelsen fremstår det tydelig hvor markant forskjellig strafferamme- og kompetansekravet for innhenting av trafikkdata blir i forhold til hva som gjelder ved innhenting av andre bevis. Pålegg om utlevering av trafikkdata blir "opphøyd" til et tvangsmiddel som står i en særstilling, og trafikkdata "opphøyes" til en type bevis som bare kan benyttes i særlige tilfeller. Den politiske debatten har vært preget av en uriktig oppfatning av at direktivet handler om innføring av en ny politimetode, og en økende bruk av tvangsmidler i etterforskningen. Ved å foreslå en ny hjemmel i straffeprosessloven som eksplisitt gjelder trafikkdata, og som har både strafferammekrav og kompetansekrav som skiller seg fra alle andre typer bevis som innhentes i straffesaker, forsterkes dette feilaktige inntrykket, og skaper en ubalanse i lovverket

En sammenligning med kravene til innhenting av lagret informasjon hos banker og finansinstitusjoner er fraværende i høringsnotatet. Selv om dette er informasjon som i utgangspunktet lagres også av andre hensyn enn de datalagringsdirektivet oppstiller, er både bevisets karakter og måten det innhentes på sammenlignbart. Innhenting av historiske data om en persons bruk av bankkort vil gi politiet noe av den samme informasjonen som trafikkdata gir.

Ved lov av 25. juni 2004 nr.52 ble påtalemyndigheten tillagt primærkompetansen til å pålegge utlevering av dokumenter og andre "*ting*" fra banker og finansinstitusjoner, jfr strpl § 230 tredje ledd. Noe av begrunnelsen var at ansatte i banker og finansinstitusjoner kun hadde "*svak taushetsplikt*"; de var ikke omfattet av strpl § 118, og hadde ikke taushetsplikt overfor retten. Dette til forskjell fra teletilbyderne, som er omfattet av § 118.

I forarbeidene har høringsinstansene og departementet vurdert flere av de samme problemstillinger som nå skal vurderes i tilknytning til innføringen av datalagringsdirektivet, blant annet om trafikkdata kan innhentes i saker hvor det (ennå) ikke foreligger mistanke mot en bestemt person for en straffbar handling. Det er relevant å se hen til disse forarbeidene både med tanke på hvem som i framtiden skal ha kompetanse til å beslutte innhenting av trafikkdata og på hvilke vilkår slike data kan innhentes.

Fra Ot.prp.nr.59 (2003-2004), kapittel 10, merknader til endringen i strpl § 210, hitsettes følgende:

> *"Etter departementets forslag til nytt tredje ledd skal påtalemyndigheten kunne pålegge vitner som nevnt i § 230 annet ledd, å utlevere dokumenter eller andre ting som antas å ha betydning som bevis, og som omfattes av forklaringsplikten for politiet. Se nærmere om forklaringsplikten etter § 230 annet ledd i de spesielle merknadene til denne bestemmelsen.*
> *Begrepet « dokumenter eller andre ting » skal forstås på samme måte som « ting » i bestemmelsens første ledd. Et pålegg om utlevering kan derfor også knytte seg til opplysninger som er lagret elektronisk, for eksempel om telefonsamtaler eller bevegelser på en bankkonto.*
>
> *Normalt kan et pålegg om utlevering etter bestemmelsens tredje ledd bare gis i straffesaker hvor det allerede er åpnet etterforskning, jf plasseringen i lovens kapittel 18 om etterforskning. Dette gjelder likevel ikke uten unntak. Dersom sterke allmenne hensyn tilsier at utlevering skjer, kan pålegg om utlevering gis uten hensyn til om det er åpnet etterforskning i straffesak, jf tredje ledd annet punktum. Unntaket tar særlig sikte på forsvinningssakene, jf merknadene til § 230 annet ledd."*

Fra merknadene til endringene i § 230 hitsettes følgende:

> *"Departementets forslag til nytt annet ledd første punktum innebærer at det innføres en forklaringsplikt overfor politiet for personer som er underlagt taushetsplikt etter sparebankloven § 21, forretningsbankloven § 18, forsikringsvirksomhetsloven § 1-3, finansieringsvirksomhetsloven § 3-14, verdipapirhandelloven § 9-8 eller verdipapirregisterloven § 8-1. Forklaringsplikten slår igjennom overfor den lovpålagte taushetsplikten etter de nevnte bestemmelser, men også overfor eventuelle avtalebestemmelser om taushetsplikt, jf henvisningen til « taushetsplikten eller taushetsplikt etter avtale ». Forklaringsplikten slår derimot ikke igjennom i forhold til annen lovpålagt taushetsplikt, jf også det som etter utkastet skal være fjerde ledd i § 230 (dagens tredje ledd).*
>
> *Forklaringsplikten inntrer først når det er åpnet etterforskning i en konkret straffesak. Dette følger av bestemmelsens plassering i lovens kapittel 18 om etterforskning. Forklaring og annen overlevering av informasjon ved mistanke om lovbrudd i saker hvor det ennå ikke er innledet etterforskning, må eventuelt skje med hjemmel i hvitvaskingsloven. Utgangspunktet om at forklaringsplikten bare gjelder i straffesaker, kan fravikes. Også i andre saker inntrer det en forklaringsplikt dersom sterke allmenne hensyn tilsier at forklaring gis, jf annet ledd annet punktum. Dette alternativet tar først og fremst sikte på å åpne for formidling av opplysninger til politiet i forsvinningssaker, hvor det kan være grunn til å frykte at noe har tilstøtt den forsvunne. Allerede i dag kan man i en del av disse sakene gi politiet opplysninger ut fra nødrettsbetraktninger, jf straffeloven § 47. Departementet ønsker imidlertid en klar regel om at personer som utfører arbeid for finansinstitusjoner mv., ikke bare kan - men også plikter - å gi politiet opplysninger i slike saker, uten at dette innebærer et brudd på den ansattes taushetsplikt etter lov eller avtale."*

Fra departementets vurdering i punkt 8.5.1 om behovet for de foreslåtte endringer hitsettes følgende:

> *"Høringen har styrket departementet i synet på at det er behov for lovendringer som gir personer som utfører arbeid for banker, forsikringsselskaper og andre finansinstitusjoner anledning til å bistå politiet med opplysninger, uten at det er nødvendig med rettens medvirkning."*
>
> *Det er først og fremst prosessøkonomiske årsaker som tilsier at personer som utfører arbeid for finansinstitusjoner mv., bør kunne videreformidle opplysninger til politiet, uten hinder av taushetsplikten. Dagens ordning fremstår etter departementets oppfatning som unødvendig ressurs- og tidkrevende. De foreslåtte lovtiltakene antas å ha en positiv effekt på tempoet og effektiviteten både i etterforskningsfasen og i andre ledd av straffesakskjeden. I tillegg til den rettsøkonomiske gevinsten som ligger i at det frigjøres ressurser i politiet, påtalemyndigheten og domstolene, vil lovtiltakene gjøre politiet i stand til raskere å innhente informasjon. I mange saker kan det være av avgjørende betydning å få innhentet informasjon hurtig, for eksempel om bruk av bankkort.*
>
> *Flere høringsinstanser, blant disse riksadvokaten og ØKOKRIM, har gitt uttrykk for at dagens ordning først og fremst fremstår som et formelt hinder for å innhente opplysninger under etterforskningen. Departementet er i det vesentlige enig i dette. De berørte gruppene plikter allerede etter gjeldende rett å forklare seg under rettslige avhør, samt å utlevere dokumenter og andre bevisgjenstander etter pålegg fra retten.*
>
> *Selv om noen vitner trolig vil føle seg mer komfortable med å avgi forklaring for retten, kan departementet ikke se at det er betenkelig ut fra et rettssikkerhetsperspektiv å gi politiet anledning*

til å gjennomføre avhør av vitner med taushetsplikt etter banklovgivningen eller annen tilsvarende særlovgivning, uten at det finner sted en slik begrenset rettslig prøvelse som straffeprosessloven § 237 gir anvisning på. Retten plikter uansett å etterkomme en begjæring om rettslig avhør, med mindre den finner at det forhold som etterforskingen gjelder, ikke er straffbart, at straffansvaret er falt bort, eller at det ikke er lovlig adgang til å ta begjæringen til følge."

Ved en implementering av datalagringsdirektivet i norsk rett kan en ikke se bort fra disse vurderingene. Dette særlig fordi trafikkdata er et bevis det allerede har vært mulig å benytte i etterforskningsøyemed her i landet siden 90-tallet, og hvor vilkår og kompetanse for innhenting for lengst er innarbeidet i eksisterende straffeprosessuelle hjemler.

På denne bakgrunn foreslås prinsipalt at det ikke foretas noen endringer i nåværende § 210 første ledd, men at trafikkdata omfattes som før. Dersom lovgiver velger en løsning med et generelt strafferammekrav i kombinasjon med spesielt angitte lovbud, må det som nevnt foretas en konkret vurdering av hvert enkelt straffebud i norsk rett. En annen løsning vil være å oppstille et lavere strafferammekrav. Men i så fall må det være så lavt som 1 års fengsel; i motsatt fall vil noen av de straffebud som omfattes av høringsnotatets forslag til ny §210 første ledd falle utenom. Sett på bakgrunn av Kripos sitt saklig begrensede ansvarsområde finner en det ikke riktig å gå nærmere inn på en vurdering av det generelle strafferammekravet eller hvilke konkrete straffebud som skal omfattes. En vil imidlertid påpeke at strafferammen ikke nødvendigvis gjenspeiler viktigheten av å oppklare en handling eller det samfunnsmessige problemet den type handlinger utgjør. Handlinger som isolert sett framstår som mindre alvorlige, eller hvor det av andre grunner ikke er aktuelt med særlig strenge straffer kan representere et samfunnsmessig problem som rettferdiggjør den type inngrep lagring og innhenting av trafikkdata representerer. Et eksempel kan være internettrelaterte overgrep begått i barne- og ungdomsmiljø hvor både gjerningsmann og offer er noenlunde jevngamle, som spredning av personlige foto/video mv.

For å sikre at også stedsspesifikke trafikkdata kan innhentes, må lovteksten formuleres slik:

"…Retten kan likevel bare pålegge besitteren å utlevere data som er lagringspliktige etter ekomloven §2-8 annet ledd så fremt det er skjellig grunn til mistanke om en handling eller forsøk på en handling som …."

Når det gjelder forslaget om at trafikkdata kun kan innhentes ved rettslig utleveringspålegg (og ikke lenger ved beslag), vil det ikke være behov for endringer i lovteksten. Det anses tilstrekkelig at det forutsettes i forarbeidene at det kun er § 210 som skal benyttes til å innhente denne type bevis. Da vil påtalemyndighetens praksis med å benytte beslagshjemmelen bortfalle. Videre foreslår Kripos som nevnt at påtalemyndigheten også i framtiden skal ha en sekundær "hastekompetanse". Dette framgår allerede av § 210 annet ledd.

6.2 Kommentarer til ekomloven § 2-8 nytt annet ledd

Dersom lovgiver beslutter at tilgangen til trafikkdata fortsatt skal gjelde alle typer lovbrudd, ikke bare de med minimum 3 års strafferamme, foreslås fjernet ordet "alvorlige" i første setning.

Som redegjort for i punkt 6.1 ovenfor foreslår Kripos – ut fra eget behov - en lagringstid på 12 måneder, som i så fall må framgå eksplisitt av lovteksten.

6.3 Kommentarer til ekomloven § 2-9 nytt femte ledd

Som Metodekontrollutvalget har drøftet i NOU 2009:15 kap. 20, vil domstolskontrollen gjøre at behovet for en forutgående prøving av PT bortfaller. En viser i denne forbindelse til at retten i medhold av strpl § 118 annet ledd uansett har kompetanse til å overprøve avgjørelsen fra PT. I så fall må ekomloven § 2-9 endres slik at det ikke gjelder noen taushetsplikt for trafikkdata som omfattes av lagringsdirektivet. Dersom lovgiver velger å følge Kripos sin anbefaling om at hastekompetansen etter § 210 skal gjelde også for trafikkdata, kan ordlyden eksempelvis formuleres slik:

"Taushetsplikten er heller ikke til hinder for at andre data enn de som er nevnt i tredje ledd utleveres til påtalemyndigheten eller politiet dersom det foreligger utleveringspålegg i medhold av strpl § 210".

DEL VII - Type data som skal lagres og lagringsløsning

Kripos vil innledningsvis påpeke viktigheten av at bestemmelsene for lagringsløsningen, både når det gjelder hvilke data som skal lagres og hvor data skal lagres, utformes på en slik måte at den fremtidige teknologiutviklingen ikke reduserer effekten av lagringen. En for eksplisitt fastsetting av hvilke data som skal lagres *kan* få en slik utilsiktet virkning. For eksempel vil "*data som er nødvendig for å spore og identifisere kilden til en kommunikasjon*" (Art. 5) sannsynligvis være helt andre data om kun få år[53]. En formålsstyrt og mest mulig teknologinøytral implementering anses avgjørende.

7.1 Data som skal lagres

Høringsnotatets pkt 4.4.1 – 4.4.5 lister opp hvilke typer data som forutsettes lagret ved en implementering av direktivet. I det alt vesentlige fremstår de presiseringene som er gjort til hver kategori av data som hensiktsmessige og riktige. I hvert fall gjelder dette på kategorier av data som allerede i dag lagres, og der dagens ordning synes å ha vært et utgangspunkt for presiseringene.

Imidlertid gjenstår en del uklarheter knyttet til kategorier som i dag ikke lagres, eller som ikke lagres fullt ut slik direktivet krever.

7.1.1 Særlig om pkt 4.4.3 – IP-telefoni

De vanligste formene for IP-telefoni vil være godt dekket, da de stort sett opererer innenfor en nasjonal nummerplan og er en del av det tradisjonelle offentlige telenettet. Ved andre former for IP-baserte løsninger (eks. Skype) vil dette imidlertid være langt mer problematisk. PT opererer med tre ulike kategorier av IP-telefonitjenester (kategori 1, 2 og 3), der bare kategori 3 (løsning som er fullstendig tilrettelagt for alle-til-alle-kommunikasjon) er regulatorisk ansett som offentlig kommunikasjonstjeneste. En presisering av lagringsplikten knyttet til de ulike kategorier av IP-telefoni vil være nødvendig blant annet for å klargjøre hvem som skal lagre hvilke opplysninger.

[53] Selv med dagens løsning for lagring av trafikkdata er kan det være et problem å spore kilden til kommunikasjon. I en drapssak fra Romerike pd (2010) ble det ved undersøkelser av trafikkdata fra offerets telefon avdekket at hun hadde mottatt flere sentrale tekstmeldinger fra et nummer angitt som "92001000" som er Netcoms tekstmeldingssentral. Hvem som faktisk var avsender fremkom ikke av listene. Undersøkelser viser at utveksling av informasjon mellom Tele2 og NetCom i disse tilfellene ikke fungerer, og at avsender av tekstmeldingen ikke blir oppgitt. Tele2 kan med dagens regelverk ikke pålegges å overføre denne informasjonen til NetCom. Tele2 har kun behov for informasjonen av hensyn til sine interne fakturerings- og driftshensyn.

7.1.2 Særlig om pkt 4.4.4 – Internettaksess

De data som skal lagres for Internetteksess vil dekke politiets behov for å identifisere abonnent til en IP-adresse på et gitt tidspunkt. Dette er det primære behov i dag. Til forskjell fra de øvrige kategoriene skal ikke mottaker eller endepunkt for kommunikasjonen lagres da dette i stor grad vil identifisere innhold, eller i hvertfall *type* innhold. Ved ikke å lagre noen som helst informasjon om mottaker eller type innhold, eller i det minste tilrettelegge for slik lagring, vil man imidlertid kunne se for seg fremtidige utfordringer som følge av teknologiutviklingen. Det er god grunn til å tro at man vil få en stadig større forskyvning av kommunikasjonsformer bort fra de klart definerte formene som telefoni, e-post osv., til det som i denne sammenheng må kategoriseres som internettaksess. Poenget er at de data som er forutsatt lagret for internettaksess *i dag* er tilstrekkelig for å ivareta intensjonen, men at det må tas høyde for at nye behov melder innen rimelig kort tid. Hvilke behov kan man ikke si med sikkerhet nå.

Eksempelvis kan nevnes at Danmark har implementert direktivet slik at et utvalg av datapakker i internett-trafikken lagres, slik at det bl.a blir mulig å identifisere kommunikajons*type*. Alternative måter å sikre teknologinøytralitet kan utredes.

7.1.3 Særlig om pkt 4.4.5 – E-post

Data knyttet til kommunikasjon med e-post er den kategorien det er størst uklarhet omkring. Problematikken knyttet til tilbyderbegrepet er ett forhold. Drøftingen i høringsnotatet berører de ulike sidene ved dette, men konkluderer ikke. Et annet forhold som vil skape utfordringer er registreringsrutiner ved opprettelse og registrering av e-postadresser hos tilbydere. Disse tjenestene faktureres ofte ikke, og det er ingen krav til legitimering eller andre former for verifisering av identitet. Slike "anonyme" e-postadresser kan sammenliknes med uregistrerte kontantkort, og medføre de samme utfordringene under politiets etterforskning.

Kripos mener at skillet mellom bredbåndstilbyderne som leverandør av e-posttjenester på den enes siden, og de web-baserte e-posttilbyderne som ikke er i kategorien bredbåndtilbydere på den andre siden er uhensiktsmessig. Et slikt skille er delvis basert på valg av teknologi, og kan ikke sies å være i tråd med direktivets intensjoner[54].

7.2 Ulike løsninger for lagringssted

Kripos er av den oppfatning at en sentralisert lagring best ivaretar politiets ulike behov.

Det vises for øvrig til ptk 4.1 hvor det er henvist til en løsning med sanntidskryptering som vil redusere de personvernmessige betenkelighetene til et absolutt minimum. Dette får også konsekvenser for valg av lagringssted. Kripos anbefaler at det velges en slik kryptert lagringsløsning. Dette vil innebære at valg av et sentralisert lagringssted ikke er betenkelig. Det vil i så fall bli samlet store mengder uleselige data som ikke gir noen mening før det foreligger en rettslig kjennelse som gir politiet tilgang til et uttrekk av dataene (dataene som kjennelsen omfatter).

Kripos mener at flere hensyn taler for sentralisert lagring.

[54] Bredbåndstilbydere tilbyr også web-basert e-post

7.2.1 Ett kontaktpunkt

Når det gjelder telefoni har man foreløpig et beskjedent antall tilbydere å forholde seg til. PTs siste oversikt over tilbydere av internettaksess viser derimot at politiet må forholde seg til over 230 tilbydere. Tilbydere av rene e-postløsninger er ikke medregnet i dette tallet. Politiet har allerede i dag en betydelig utfordring i å holde oversikt over kontaktpunkter for disse, og man ser at antallet tilbydere er voksende både for telefoni, internettaksess og e-post. En sentralisert lagring vil gi ett kontaktpunkt for denne typen anmodninger, og vil innebære en betydelig ressursbesparelse for politiet. I høringsnotatet fremholdes politiets utfordringer på dette området i forbindelse med kommunikasjonskontroll, og at det blir "viktig å finne løsninger som forenkler den praktiske prosessen". Kripos er av den oppfatning at en sentralisert lagring *er* en slik løsning, og mener at en lagring hos tilbyderne ikke kan foretrekkes uten at man har funnet tilfredsstillende løsninger på dette området.

7.2.2 Tilgjengelighet

Direktivet legger opp til at data skal kunne utleveres uten unødvendig forsinkelse. Kripos er av den oppfatning at data som er forutsatt lagret, i gitte tilfeller bør være tilgjengelig for utlevering på 24/7-basis. Selv om et sentralt lagringssted ikke nødvendigvis vil ha "live" tilgang til opplysningene (nødrettssaker), vil en sentralisert lagring kunne sikre tilgang til opplysningene senest inne ett døgn (jfr. Teleplans utredning). Svært mange tilbydere kan i dag ikke møte et slikt behov, og det vil også for svært mange være urealistisk å etablere og drifte et slikt tilbud. De skisserte formene for mellomløsning vil kunne være et alternativ, men medfører ingen garanti ved frivillighet.

7.2.3 Integritet

Ett sentralt lagringssted vil sikre en enhetlig form for lagring, samt at data kan utleveres i henhold til standardiserte prosedyrer og i standardiserte formater. Dette vil medføre en betydelig lettelse i bearbeidingen av dataene, samt at det på en bedre måte sikrer at lagring og utlevering av dataene er i henhold til bestemmelsene i direktivet. Enhetlig format på data som utlevers vil muligens kunne ivaretas ved lagring hos tilbyder eller ved mellomløsninger, mens enhetlige prosedyrer for utlevering neppe kan ivaretas like godt om ansvaret for dette overlates til så mange tilbydere.

En annen utfordring knyttet til å identifisere kilden for kommunikasjon er en økende grad av fragmentert lagring av data. Dette vil være data som i sum er nødvendige for identifisering. Det er fremholdt som et prinsipp at data kun skal lagres en gang (ett sted) og følgelig må data innhentes fra flere kilder for å oppnå ett formål. Teknologiutviklingen og nisjemessige forutsetninger i bransjen vil trolig forsterke denne utviklingen. Ett lagringssted vil både møte kravet om lagring en gang, og behovet for en effektiv tilgang til nødvendige data.

7.2.4 Politiets behov for konfidensialitet

Politiet er i mange sammenhenger er avhengig av konfidensialitet rundt de etterforskningsskritt som gjennomføres, herunder innhenting av trafikkdata. Manglende konfidensialitet vil medføre at formålet med etterforskningen forspilles ved at mistenkte får kjennskap til politiets etterforskning. Dette gjelder for så vidt både åpen og skjult etterforskning.

Ett lagringssted som er uavhengig av tilbyderne vil medføre en åpenbart bedre sikkerhet mot at uvedkommende får kunnskap om de etterforskningsskritt politiet har iverksatt. Lekkasje av slik informasjon kan selvsagt både skje forsettlig fra noen som ser seg tjent med

det, men kan også skje uforvarende eller ved en tilfeldighet. Det kan uansett være til stor skade for etterforskningen. At 230 tilbydere skal ekspedere slike henvendelser fra politiet medfører en åpenbart større risiko for slike lekkasjer. Det finnes flere eksempler på at problemstillingen er reell.

Kravet om at kun autorisert personell har tilgang til opplysningene gir ingen selvstendig garanti for konfidensialitet. At slikt personell må autoriseres hos så mange forskjellige tilbydere innebærer en større risiko enn om både autorisasjon og kontroll med autorisert personell sentraliseres.

7.2.5 Tilsyn, kontroll, statistikk og rapportering

Det er også et vesentlig poeng med innføringen av direktivet at kontroll med lagring og utlevering av opplysningene er streng og god. Videre er det et krav om rapportering av antallet imøtekomne anmodninger, tiden mellom lagringstidspunkt og etterspørsel samt antallet saker der anmodningene ikke er imøtekommet.

I tillegg til å lette kontrollen betraktelig, er det også nærliggende å tro at kvaliteten på selve kontrollen vil bli bedre med en slik løsning. Ett lagringssted (og behandlingssted) vil også sikre en mer enhetlig og fullstendig statistikk, slik direktivet krever.

Høringsbrevet skisserer en todelt tilsynsordning delt mellom Post- og teletilsynet og Datatilsynet. Kripos har i høringsuttalelse til NOU 2009:1 – "Individ og integritet" stilt spørsmål med om ikke rollen som ombud og tilsyn bør skilles da blandingen av disse rollene åpenbart kan være problematisk. Høringsuttalelsen fremgår i vedlegg 2. Det vises særlig til pkt 4.

7.2.6 Krav til sikkerhet/personvernhensyn

Høringsnotatet støtter seg til Datatilsynets innvendig mot sentralisert lagring når det gjelder den personvernrisiko dette medfører. Dette resonnementet synes utelukkende å basere seg på skadepotensialet ved et sikkerhetsbrudd, og i liten grad sannsynligheten for selve bruddet. Skadepotensialet ved enkeltbrudd er åpenbart større om alle data lagres på ett sted.

Likevel har ikke høringsnotatet drøftet denne problemstillingen opp mot en løsning med sanntidskryptering av data, se pkt 4.1. Som nevnt tidligere er ikke en kryptert lagringsløsning omhandlet i høringsnotatet eller i de forutgående utredningene. Kripos finner dette merkelig da en kryptert løsning vil øke sikkerheten rundt de lagrede data i meget stor grad.

Kripos anbefaler en kryptert lagringsløsning. Men skulle man av ukjente årsaker velge en ukryptert løsning, så er faren for at flere sikkerhetsbrudd inntreffer er like åpenbart større om man overlater lagring og utlevering til et stadig økende antall tilbydere.

Ved å velge ett sentralt lagringspunkt vil myndighetene også ha en betydelig bedre mulighet til å påvirke valget av lagringsløsning, slik at sikkerhetshensyn derved kan få høyere vekting enn kostnader og ordinær drift. Dette, kombinert med enklere og bedre kontroll og tilsyn, bør mer enn veie opp for det faktum at et sikkerhetsbrudd ved en sentralisert løsning vil få større konsekvenser.

Høringsnotatet[55] legger også opp til at teletilbyderne selv skal få velge hvorvidt de ønsker å lagre data selv eller å be en tredjepart foreta lagringen for dem. Videre fremgår det at det er "*sannsynlig at det på kommersielt grunnlag vil oppstå løsninger hvor mindre tilbydere tilbys felles lagring*". Kripos er skeptisk til en løsning hvor teletilbydernes kostnadsvurderinger åpenbart vil ligge til grunn for valg av lagringsløsning. Resultatet av en slik løsning er at man kan få en kommersiell tilbyder som lagrer trafikkdata for alle tilbyderne unntatt de store tilbyderne som allerede har etablerte systemer for denne typen lagring. Dette vil innebære en valgfri form for mellomløsning der kostnadsaspektet er den drivende faktoren. De prinsipielle og sikkerhetsmessige diskusjonene om sentral eller desentralisert lagring overlates til den enkelte tilbyder, noe som etter Kripos' syn er uheldig.

Kripos støtter forslaget om at lagringen skal foretas av *en* objektiv tredjepart, eksempelvis gjennomført ved at bransjen selv pålegges å etablerer en løsning for sentralisert lagring som underlegges nødvendig kontroll.

Videre legges det opp til et krav om at data som lagres for politiets bruk skal lagres atskilt fra de data som lagres for fakturerings-, kommunikasjons- og driftsformål. En sentralisert lagring vil i seg selv ivareta et slikt krav.

Det argumenteres med at en sentralisert lagring betinger at man sikrer seg at dataene ikke blir brukt til andre formål enn de er ment for, og at dette er vanskelig på grunn av at det alltid foreligger en viss fare for utilsiktet utlevering eller misbruk. Kripos kan ikke se at en lagring hos tilbydere sikrer dette på en bedre måte, eller at fare for utilsiktet utlevering eller misbruk blir mindre. Basert på argumentasjonen over mener Kripos tvert imot at en *sentralisert og kryptert lagring* ivaretar disse hensyn best.

DEL VIII - Sammendrag / oppsummering

Politiet har benyttet trafikkdata i etterforskningen siden 90-tallet. Trafikkdata er godt etablert som en av politiets viktigste verktøy i etterforskning av alvorlig kriminalitet. Det vises til gjennomgangen av politiets bruk av trafikkdata og vurderingen av nytteverdien i etterforskning i henholdsvis *del II* og *del III* av høringssvaret.

Det finnes ikke noe alternativ til trafikkdata i "politiets verktøykasse". Trafikkdata er en av få objektiv kontrollerbare bevis i mange etterforskninger. Sikringspålegg etter strpl §215a kan i liten grad reparere manglende lagring da dette krever både at trafikkdata faktisk lagres for at det skal være noe å "fryse" og at politiet allerede i starten vet hvilke data som er relevante. Det siste er sjeldent tilfelle.

Trafikkdata har så langt vært lagret ut fra teletilbydernes interne behov, og dette behovet er nå i ferd med å forsvinne. For IP-data er det allerede en meget mangelfull lagringspraksis som resulterer i at alvorlige saker ikke oppklares. For politiet er det meget viktig at det nå sikres at trafikkdata også for fremtiden fortsatt vil være tilgjengelige for politiets behov ved at det innføres en lagringsplikt for tilbyderne. Innføringen av EUs datalagringsdirektiv er en meget godt egnet måte å gjøre dette på. Dette vil skape en forutsigbarhet for hvilke data som skal være tilgjengelig for politiets etterforskning. Kripos anbefaler derfor sterkt at direktivet innføres.

[55] Høringsnotatet, pkt 4.7 – særlig pkt 4.7.3 og 4.7.4.5

Kripos mener at en lagringstid på minst 1 år for trafikkdata fremstår som en fornuftig avveining av både personvernhensyn og politiets behov for lagring innenfor Kripos' ansvarsområde. Kripos anbefaler at det ikke skilles i lagringstid for telefon- og IP-trafikk.

De foreslåtte nasjonale bestemmelsene om politiets tilgang til trafikkdata medfører en kraftig innskjerping av dagens praksis. Kripos mener prinsipalt at det ikke bør innføres et strafferammekrav på 3 års fengsel. Dette vil avvike fra de øvrige bestemmelsene i straffeprosessloven om innhenting av bevis. Subsidiært må det gjøres unntak for blant annet etterforskning etter strpl §224, 4.ledd (ulykker), saknetsaker og redningsaksjoner. Videre må det gjøres en nøye gjennomgang av hvilke straffebud i både straffeloven og særlovgivningen som skal særskilt opplistes i kategorien "særlige saker".

Videre mener Kripos at kravet om at "*noen mistenkes*" ikke bør innføres. Dette vil utelukke viktige stedsspesifikke trafikkdata som er av stor betydning for etterforskning av en rekke sakstyper.

Det må også gis hastekompetanse for påtalemyndigheten for innhenting av trafikkdata, på samme måte som det er for øvrige tvangsmidler.

Dersom direktivet ikke innføres, eller at det legges for begrensende nasjonale føringer på lagringstid og politiets tilgang til data, er det utvilsomt at en rekke alvorlige straffesaker ikke vil oppklares. Dette sett hen til betydningen av trafikkdata i etterforskning av alvorlig kriminalitet. Politiet vil således ikke kunne innfri de forventninger samfunnet og fornærmede har til at sakene skal oppklares.

Høringsnotatet skisserer flere løsninger for tilbydernes lagring av trafikkdata. Det sentrale er at det velges en lagring med sanntidskryptering av alle lagrede data. Dette vil redusere de personvernmessige betenkelighetene til et absolutt minimum. Kripos mener at en sentralisert og kryptert mellomløsning er beste løsning, både av hensyn til sikring av data, politiets behov for tilgang til data og krav til konfidensialitet. Kripos anbefaler ikke at det skal være opp til tilbyderne å velge lagringsløsning. Dette vil medføre at kostnadsspørsmål vil være den drivende faktoren fremfor viktige spørsmål som sikring av data og politiets behov for tilgang til data.

Kripos mener at de forslagene til hvilke data som skal lagres i det vesentlige fremstår som hensiktsmessige og riktige. Det er imidlertid viktig å avklare uklarheter knyttet til noen av kategoriene av data som foreslått lagret, se pkt 7.1. Det er viktig at det innføres teknologinøytrale regler for lagring som også ivaretar at nye behov som melder seg innen rimelig kort tid.

Med hilsen

Odd Reidar Humlegård
Sjef Kripos

Vedlegg:

1. *Kripos' undersøkelse mars 2010: Politiets bruk av trafikkdata*
2. *Høringssvar fra Kripos NOU 2009:1- "Individ og integritet"*

Kopi: Politidirektoratet

Saksbehandlere:	Pob Rune Utne Reitan	Padv Anne Cecilie Dessarud
Tlf.:	23208665	23208960

POLITIET

Kripos' undersøkelse mars 2010:

Politiets bruk av trafikkdata

Metode for spørreundersøkelsen om bruk av historiske trafikkdata i etterforskning

Innledning

Kripos ønsket å belyse i hvilken utstrekning trafikkdata blir brukt i etterforskningen av alvorlig kriminalitet, siden det per i dag ikke finnes offentlig statistikk over dette, som et innspill til Politidirektoratet i høringen om Datalagringsdirektivet.

Utvalget

Kripos gjennomførte mars 2010 en undersøkelse vedrørende bruk av trafikkdata i norsk politi innenfor etterforskning av utvalgte typer alvorlig kriminalitet, herunder drap (strl § 233), narkotika (strl § 162, 2. og 3. ledd), grovt ran (strl § 268, jf § 267), voldtekt (strl §192) og seksuell omgang med barn u/10 år og u/14 år (strl § 195). Statistikkgruppene er hentet fra Strasakregisteret, som fører oversikt over alle straffesaker i Norge og danner grunnlag for offentlig kriminalstatistikk. De utvalgte statistikkgruppene er ment å vise høyt prioriterte sakstyper i politiet. Samtidig gjenspeiler de sakstypene som Post- og Teletilsynet hvor de hyppigst gir fritak fra taushetsplikten[1]. Undersøkelsen omfatter alle saker innenfor disse statistikkgruppene hvor det er fattet en positiv påtalebeslutning, totalt 1450 saker.

Avgrensning

Vi har avgrenset mot saker som fortsatt (per 25. februar 2010) er under etterforskning, og hvor det av den grunn kanskje ikke ville være mulig å besvare alle spørsmålene. Vi har også avgrenset mot alle saker som har endt med henleggelse, uavhengig av henleggelseskode. I hvilken grad det har vært foretatt etterforskningsskritt i de henlagte sakene varierer mye. Eksempelvis kan det være at en allerede ved mottak av anmeldelse beslutter å ikke iverksette etterforskning. På den andre side kan det være tilfeller hvor det har pågått en omfattende etterforskning, men hvor påtalemyndigheten ikke har funnet tilstrekkelig grunnlag for å ta ut tiltale. Om og i hvilken grad de henlagte sakene har vært etterforsket, og om det omfatter innhenting av samtaledata, framgår naturlig nok ikke av statistikken. Henleggelseskoden gir heller ikke svar på dette. For å unngå feilkilder har vi derfor avgrenset mot alle henlagte saker.

Tidsaspektet

Sett hen til den tid som var til rådighet og vår mulighet til å ferdigstille undersøkelsen og bearbeide resultatene tidsnok til at de kunne medtas som en del av høringsuttalelsen, har vi avgrenset undersøkelsen til å omfatte saker som ble registrert i perioden 01.01.2008 til 31.12.2008. 2008 er valgt fordi det ligger så vidt kort tilbake i tid at respondentene

[1] Brev av 08.12.09 fra Post- og teletilsynet til Justis og politidepartementet, PT-ref 0906631-2

formentlig husker hvilke vurderinger som ble gjort under etterforskningen, samtidig som det ligger langt nok tilbake i tid til at de fleste av sakene er ferdig etterforsket og påtaleavgjort.

Metode
Vi fant det hensiktsmessig å sende ut et elektronisk strukturert spørreskjema, ved å bruke verktøyet Questback. Spørsmålene ble utarbeidet av representanter fra Taktisk etterforskningsavdeling ved Kripos, med teknisk bistand fra Questback.

Det ble sendt ut personlig mail til hovedetterforsker med henvisning til rolle, saksnummer, registreringsdato for saken og sakskategori, for å sikre oss at respondentene svarte på konkrete saker og ikke gav en generell tilbakemelding. I de saker hvor det ikke var registrert en hovedetterforsker i Strasak, ble mailen sendt til påtaleansvarlig i saken. Koblingen mellom sakskategori og etterforsker/påtalejurist ble hentet fra Strasak registeret.

For å få et innblikk i bruken av historiske trafikkdata i alvorlige straffesaker i 2008, spurte vi om det ble innhentet trafikkdata i den konkrete saken. Vi bad om etterforsker/påtalejuristens vurdering, ut fra en skala fra en til fem, av i hvilken grad trafikkdata bidro med informasjon av betydning for etterforskningen av saken, og hvilke opplysninger trafikkdata bidro med ut fra gitte kriterier. I de saker hvor det ikke var innhentet trafikkdata spurte vi respondentene om årsaken til at det ikke var blitt gjort, ut fra gitte kriterier. Til slutt bad vi om en vurdering av om det ville vært relevant å innhente historiske trafikkdata lengre tilbake i tid i den konkrete saken om det hadde vært mulig, se vedlegg 2.

Undersøkelsen ble sendt ut 3. mars 2010 og var tilgjengelig for respondentene til 12. mars, 8 arbeidsdager. 2 respondenter meldte om feilkodede saker i Strasak registeret. De nevnte sakene ble slettet fra undersøkelsen. Svarprosenten var på 67 %. Det kan bemerkes at undersøkelsen ble sendt ut i vinterferien for østlandet.

Kripos ønsker å påpeke at funn fra undersøkelsen ikke gir et fullstendig bilde av bruken av trafikkdata i alvorlige kriminalsaker. Målingen viser hvor ofte trafikkdata ble innhentet i alvorlige straffesaker ut fra utvalgte kategorier i 2008 av saker med positiv påtalebeslutning, og hva de enkelte hovedetterforskerne/påtalejuristene har ment om betydningen av trafikkdata i deres konkrete sak.

Kripos, 15.03.10

Vedlegg:
Resultater fra undersøkelsen:
- *alle kategorier samlet*
- *drapssaker*
- *grove narkotikasaker*
- *grove ran*
- *seksuelle overgrep*

Bruk av historiske trafikkdata i etterforskning

Kategori: ALLE KATEGORIER - SAMLET

Publisert fra 03.03.2010 til 12.03.2010

966 respondenter (375 unike)

2. Ble det innhentet historiske trafikkdata i forbindelse med etterforskningen av denne saken?

Alternativer	Prosent	Verdi
1 Ja, trafikkdata fra mobil-/fasttelefoni	48,8 %	471
2 Ja, IP-trafikk	0,3 %	3
3 Ja, både fra mobil-/fasttelefoni og IP-trafikk	2,8 %	27
4 Nei	48,1 %	465
Total		966

Gjennomsnitt		2,50
Standard avvik		1,48
Median		3,0

3. Hvor enig eller uenig er du i at trafikkdata bidro med informasjon av stor betydning for etterforskningen i denne saken

Alternativer	Prosent	Verdi
1 Helt uenig	8,6 %	43
2 Litt uenig	3,4 %	17
3 Verken uenig eller enig	5,6 %	28
4 Litt enig	21,8 %	109
5 Helt enig	60,7 %	304
Total		501

Gjennomsnitt		4,23
Standard avvik		1,23
Median		5,0

4. Dersom trafikkdata hadde betydning for etterforskningen i denne saken, hvilke opplysninger bidro det med? (flere svar mulig)

Alternativer	Prosent	Verdi
1 Identifisering av gjerningsperson(er)	54,2 %	224
2 Kontroll av mistenkte/siktedes bevegelser	81,8 %	338
3 Kontroll av opplysninger fremkommet i politiavhør eller andre undersøkelser	76,8 %	317
4 Kartlegge personer i et bestemt område (basestasjonsutskrifter)	34,6 %	143
5 Sjekke personer inn/ut av saken	39,5 %	163
6 Opplysninger om mistenktes/siktedes kontaktmønster (kontaktanalyse)	75,3 %	311
7 Trafikkdata var ressursbesparende for saken ved at andre metoder/undersøkelser kunne utelates	25,7 %	106
8 Annet:	4,8 %	20
Total		413

Gjennomsnitt		3,70
Standard avvik		1,96
Median		3,0

5. Hvorfor ble det ikke innhentet trafikkdata i denne saken?

Alternativer	Prosent	Verdi
1 Det ble ikke vurdert	19,4 %	90
2 Det ble vurdert, men det var ikke nødvendig for etterforskningen	64,5 %	300
3 Det ble vurdert som nødvendig, men det var for kostbart	1,9 %	9
4 Det ble vurdert som nødvendig, men data var slettet pga kort lagringstid	2,6 %	12
5 Annet	11,6 %	54
Total		465

Gjennomsnitt		2,23
Standard avvik		1,14
Median		2,0

6. Hvor enig eller uenig er du i at det ville vært relevant å innhente historiske trafikkdata lengre tilbake i tid i denne aktuelle saken med hensyn til:

I dag lagres historiske trafikkdata hos teleselskapene i henholdsvis 150 dager hos Netcom og i 90 dager hos Telenor. IP-trafikk kan lagres i 21 dager.Hvor enig eller uenig er du i at det ville vært relevant å innhente historiske trafikkdata lengre tilbake i tid i denne saken med hensyn til:

Alternativer	N
1 Trafikkdata fra mobil-/fasttelefoni	961
2 IP-trafikk	750

6.1 Hvor enig eller uenig er du i at det ville vært relevant å innhente historiske trafikkdata lengre tilbake i tid i denne aktuelle saken med hensyn til: - Trafikkdata fra mobil-/fasttelefoni

Alternativer	Prosent	Verdi
1 Helt uenig	21,5 %	207
2 Litt uenig	3,4 %	33
3 Verken uenig eller enig	15,2 %	146
4 Litt enig	9,5 %	91
5 Helt enig	50,4 %	484
Total		961

Gjennomsnitt		3,64
Standard avvik		1,61
Median		5,0

6.2 Hvor enig eller uenig er du i at det ville vært relevant å innhente historiske trafikkdata lengre tilbake i tid i denne aktuelle saken med hensyn til: - IP-trafikk

Alternativer	Prosent	Verdi
1 Helt uenig	27,5 %	206
2 Litt uenig	3,5 %	26
3 Verken uenig eller enig	24,3 %	182
4 Litt enig	4,0 %	30
5 Helt enig	40,8 %	306
Total		750

Gjennomsnitt		3,27
Standard avvik		1,65
Median		3,0

Bruk av historiske trafikkdata i etterforskning

KATEGORI: DRAP

Publisert fra 03.03.2010 til 12.03.2010

23 respondenter (22 unike)

Filter: Vold

"Statistikkgruppe" = "1708 drap ($ 233)"

"Statistikkgruppe" = "1714 legemsbeskadigelse med døden til følge ($ 229)"

2. Ble det innhentet historiske trafikkdata i forbindelse med etterforskningen av denne saken?

Alternativer	Prosent	Verdi
1 Ja, trafikkdata fra mobil-/fasttelefoni	73,9 %	17
2 Ja, IP-trafikk	0,0 %	0
3 Ja, både fra mobil-/fasttelefoni og IP-trafikk	0,0 %	0
4 Nei	26,1 %	6
Total		23

Gjennomsnitt		1,78
Standard avvik		1,32
Median		1,0

3. Hvor enig eller uenig er du i at trafikkdata bidro med informasjon av stor betydning for etterforskningen i denne saken

Alternativer	Prosent	Verdi
1 Helt uenig	11,8 %	2
2 Litt uenig	5,9 %	1
3 Verken uenig eller enig	5,9 %	1
4 Litt enig	17,6 %	3
5 Helt enig	58,8 %	10
Total		17

Gjennomsnitt		4,06
Standard avvik		1,39
Median		5,0

4. Dersom trafikkdata hadde betydning for etterforskningen i denne saken, hvilke opplysninger bidro det med? (flere svar mulig)

Alternativer	Prosent	Verdi
1 Identifisering av gjerningsperson(er)	15,4 %	2
2 Kontroll av mistenkte/siktedes bevegelser	92,3 %	12
3 Kontroll av opplysninger fremkommet i politiavhør eller andre undersøkelser	100,0 %	13
4 Kartlegge personer i et bestemt område (basestasjonsutskrifter)	30,8 %	4
5 Sjekke personer inn/ut av saken	30,8 %	4
6 Opplysninger om mistenktes/siktedes kontaktmønster (kontaktanalyse)	38,5 %	5
7 Trafikkdata var ressursbesparende for saken	38,5 %	5

	ved at andre metoder/undersøkelser kunne utelates		
8	Annet:	0,0 %	0
Total			13

Gjennomsnitt		3,69
Standard avvik		1,79
Median		3,0

5. Hvorfor ble det ikke innhentet trafikkdata i denne saken?

Alternativer		Prosent	Verdi
1	Det ble ikke vurdert	33,3 %	2
2	Det ble vurdert, men det var ikke nødvendig for etterforskningen	66,7 %	4
3	Det ble vurdert som nødvendig, men det var for kostbart	0,0 %	0
4	Det ble vurdert som nødvendig, men data var slettet pga kort lagringstid	0,0 %	0
5	Annet	0,0 %	0
Total			6

Gjennomsnitt		1,67
Standard avvik		0,47
Median		2,0

6. Hvor enig eller uenig er du i at det ville vært relevant å innhente historiske trafikkdata lengre tilbake i tid i denne aktuelle saken med hensyn til:

Alternativer		N
1	Trafikkdata fra mobil-/fasttelefoni	23
2	IP-trafikk	18

6.1 Hvor enig eller uenig er du i at det ville vært relevant å innhente historiske trafikkdata lengre tilbake i tid i denne aktuelle saken med hensyn til: - Trafikkdata fra mobil-/fasttelefoni

Alternativer		Prosent	Verdi
1	Helt uenig	21,7 %	5
2	Litt uenig	13,0 %	3
3	Verken uenig eller enig	39,1 %	9
4	Litt enig	4,3 %	1
5	Helt enig	21,7 %	5
Total			23

Gjennomsnitt		2,91
Standard avvik		1,38
Median		3,0

6.2 Hvor enig eller uenig er du i at det ville vært relevant å innhente historiske trafikkdata lengre tilbake i tid i denne aktuelle saken med hensyn til: - IP-trafikk

Alternativer	Prosent	Verdi
1 Helt uenig	33,3 %	6
2 Litt uenig	0,0 %	0
3 Verken uenig eller enig	44,4 %	8
4 Litt enig	11,1 %	2
5 Helt enig	11,1 %	2
Total		18

Gjennomsnitt		2,67
Standard avvik		1,33
Median		3,0

Bruk av historiske trafikkdata i etterforskning

KATEGORI: GROVE NARKOTIKASAKER

Publisert fra 03.03.2010 til 12.03.2010

675 respondenter (221 unike)

Filter: Narkotika

"Statistikkgruppe" = "703 narkotika ($ 162,2.ledd)"

"Statistikkgruppe" = "708 narkotika ($ 162,3.ledd)"

2. Ble det innhentet historiske trafikkdata i forbindelse med etterforskningen av denne saken?

Alternativer	Prosent	Verdi
1 Ja, trafikkdata fra mobil-/fasttelefoni	57,0 %	385
2 Ja, IP-trafikk	0,3 %	2
3 Ja, både fra mobil-/fasttelefoni og IP-trafikk	2,2 %	15
4 Nei	40,4 %	273
Total		675

Gjennomsnitt		2,26
Standard avvik		1,46
Median		1,0

3. Hvor enig eller uenig er du i at trafikkdata bidro med informasjon av stor betydning for etterforskningen i denne saken

Alternativer	Prosent	Verdi
1 Helt uenig	9,0 %	36
2 Litt uenig	2,2 %	9
3 Verken uenig eller enig	4,7 %	19
4 Litt enig	20,4 %	82
5 Helt enig	63,7 %	256
Total		402

Gjennomsnitt		4,28
Standard avvik		1,23
Median		5,0

4. Dersom trafikkdata hadde betydning for etterforskningen i denne saken, hvilke opplysninger bidro det med? (flere svar mulig)

Alternativer	Prosent	Verdi
1 Identifisering av gjerningsperson(er)	60,7 %	205
2 Kontroll av mistenkte/siktedes bevegelser	87,6 %	296
3 Kontroll av opplysninger fremkommet i politiavhør eller andre undersøkelser	76,9 %	260
4 Kartlegge personer i et bestemt område (basestasjonsutskrifter)	37,3 %	126
5 Sjekke personer inn/ut av saken	39,9 %	135
6 Opplysninger om mistenktes/siktedes kontaktmønster (kontaktanalyse)	80,8 %	273
7 Trafikkdata var ressursbesparende for saken	26,6 %	90

	ved at andre metoder/undersøkelser kunne utelates		
8	Annet:	4,1 %	14
Total			338

Gjennomsnitt	3,67
Standard avvik	1,96
Median	3,0

5. Hvorfor ble det ikke innhentet trafikkdata i denne saken?

Alternativer		Prosent	Verdi
1	Det ble ikke vurdert	13,6 %	37
2	Det ble vurdert, men det var ikke nødvendig for etterforskningen	65,6 %	179
3	Det ble vurdert som nødvendig, men det var for kostbart	3,3 %	9
4	Det ble vurdert som nødvendig, men data var slettet pga kort lagringstid	0,7 %	2
5	Annet	16,8 %	46
Total			273

Gjennomsnitt	2,42
Standard avvik	1,24
Median	2,0

6. Hvor enig eller uenig er du i at det ville vært relevant å innhente historiske trafikkdata lengre tilbake i tid i denne aktuelle saken med hensyn til:

I dag lagres historiske trafikkdata hos teleselskapene i henholdsvis 150 dager hos Netcom og i 90 dager hos Telenor. IP-trafikk kan lagres i 21 dager.Hvor enig eller uenig er du i at det ville vært relevant å innhente historiske trafikkdata lengre tilbake i tid i denne saken med hensyn til:

Alternativer		N
1	Trafikkdata fra mobil-/fasttelefoni	673
2	IP-trafikk	487

6.1 Hvor enig eller uenig er du i at det ville vært relevant å innhente historiske trafikkdata lengre tilbake i tid i denne aktuelle saken med hensyn til: - Trafikkdata fra mobil-/fasttelefoni

Alternativer		Prosent	Verdi
1	Helt uenig	16,2 %	109
2	Litt uenig	2,5 %	17
3	Verken uenig eller enig	15,2 %	102
4	Litt enig	10,0 %	67
5	Helt enig	56,2 %	378
Total			673

Gjennomsnitt	3,87
Standard avvik	1,50
Median	5,0

6.2 Hvor enig eller uenig er du i at det ville vært relevant å innhente historiske trafikkdata lengre tilbake i tid i denne aktuelle saken med hensyn til: - IP-trafikk

Alternativer	Prosent	Verdi
1 Helt uenig	23,0 %	112
2 Litt uenig	2,5 %	12
3 Verken uenig eller enig	27,1 %	132
4 Litt enig	4,1 %	20
5 Helt enig	43,3 %	211
Total		487

Gjennomsnitt		3,42
Standard avvik		1,59
Median		3,0

Bruk av historiske trafikkdata i etterforskning

KATEGORI: GROVE RAN

Publisert fra 03.03.2010 til 12.03.2010

50 respondenter (34 unike)

Filter: Ran

"Statistikkgruppe" = "2503 ran,grovt ($ 268)"

"Statistikkgruppe" = "2505 bankran ($ 268,2)"

"Statistikkgruppe" = "2506 postran ($ 268,2)"

"Statistikkgruppe" = "2510 grovt ran fra forretning/kiosk ($ 268)"

2. Ble det innhentet historiske trafikkdata i forbindelse med etterforskningen av denne saken?

Alternativer	Prosent	Verdi
1 Ja, trafikkdata fra mobil-/fasttelefoni	34,0 %	17
2 Ja, IP-trafikk	0,0 %	0
3 Ja, både fra mobil-/fasttelefoni og IP-trafikk	4,0 %	2
4 Nei	62,0 %	31
Total		50

Gjennomsnitt		2,94
Standard avvik		1,41
Median		4,0

3. Hvor enig eller uenig er du i at trafikkdata bidro med informasjon av stor betydning for etterforskningen i denne saken

Alternativer	Prosent	Verdi
1 Helt uenig	10,5 %	2
2 Litt uenig	0,0 %	0
3 Verken uenig eller enig	5,3 %	1
4 Litt enig	26,3 %	5
5 Helt enig	57,9 %	11
Total		19

Gjennomsnitt		4,21
Standard avvik		1,24
Median		5,0

4. Dersom trafikkdata hadde betydning for etterforskningen i denne saken, hvilke opplysninger bidro det med? (flere svar mulig)

Alternativer	Prosent	Verdi
1 Identifisering av gjerningsperson(er)	50,0 %	8
2 Kontroll av mistenkte/siktedes bevegelser	87,5 %	14
3 Kontroll av opplysninger fremkommet i politiavhør eller andre undersøkelser	62,5 %	10
4 Kartlegge personer i et bestemt område (basestasjonsutskrifter)	68,8 %	11
5 Sjekke personer inn/ut av saken	50,0 %	8
6 Opplysninger om mistenktes/siktedes kontaktmønster (kontaktanalyse)	50,0 %	8

7	Trafikkdata var ressursbesparende for saken ved at andre metoder/undersøkelser kunne utelates	31,3 %	5
8	Annet:	12,5 %	2
Total			16

Gjennomsnitt	3,77
Standard avvik	1,95
Median	4,0

5. Hvorfor ble det ikke innhentet trafikkdata i denne saken?

Alternativer		Prosent	Verdi
1	Det ble ikke vurdert	25,8 %	8
2	Det ble vurdert, men det var ikke nødvendig for etterforskningen	71,0 %	22
3	Det ble vurdert som nødvendig, men det var for kostbart	0,0 %	0
4	Det ble vurdert som nødvendig, men data var slettet pga kort lagringstid	3,2 %	1
5	Annet	0,0 %	0
Total			31

Gjennomsnitt	1,81
Standard avvik	0,59
Median	2,0

6. Hvor enig eller uenig er du i at det ville vært relevant å innhente historiske trafikkdata lengre tilbake i tid i denne aktuelle saken med hensyn til:

I dag lagres historiske trafikkdata hos teleselskapene i henholdsvis 150 dager hos Netcom og i 90 dager hos Telenor. IP-trafikk kan lagres i 21 dager.Hvor enig eller uenig er du i at det ville vært relevant å innhente historiske trafikkdata lengre tilbake i tid i denne saken med hensyn til:

Alternativer		N
1	Trafikkdata fra mobil-/fasttelefoni	50
2	IP-trafikk	42

6.1 Hvor enig eller uenig er du i at det ville vært relevant å innhente historiske trafikkdata lengre tilbake i tid i denne aktuelle saken med hensyn til: - Trafikkdata fra mobil-/fasttelefoni

Alternativer		Prosent	Verdi
1	Helt uenig	26,0 %	13
2	Litt uenig	6,0 %	3
3	Verken uenig eller enig	12,0 %	6
4	Litt enig	12,0 %	6
5	Helt enig	44,0 %	22
Total			50

Gjennomsnitt	3,42
Standard avvik	1,67
Median	4,0

6.2 Hvor enig eller uenig er du i at det ville vært relevant å innhente historiske trafikkdata lengre tilbake i tid i denne aktuelle saken med hensyn til: - IP-trafikk

Alternativer	Prosent	Verdi
1 Helt uenig	28,6 %	12
2 Litt uenig	7,1 %	3
3 Verken uenig eller enig	11,9 %	5
4 Litt enig	4,8 %	2
5 Helt enig	47,6 %	20
Total		42

Gjennomsnitt		3,36
Standard avvik		1,74
Median		4,0

Bruk av historiske trafikkdata i etterforskning

KATEGORI: SEKSUELLE OVERGREP

Publisert fra 03.03.2010 til 12.03.2010

218 respondenter (128 unike)

Filter: Seksualisert vold

"Statistikkgruppe" = "1401 voldtekt ($ 192,1.og 2.ledd)"

"Statistikkgruppe" = "1402 seksuell omgang med barn u/14 år ($ 195)"

"Statistikkgruppe" = "1403 seksuell omgang med barn u/10 år ($ 195)"

2. Ble det innhentet historiske trafikkdata i forbindelse med etterforskningen av denne saken?

Alternativer	Prosent	Verdi
1 Ja, trafikkdata fra mobil-/fasttelefoni	23,9 %	52
2 Ja, IP-trafikk	0,5 %	1
3 Ja, både fra mobil-/fasttelefoni og IP-trafikk	4,6 %	10
4 Nei	71,1 %	155
Total		218

Gjennomsnitt		3,23
Standard avvik		1,27
Median		4,0

3. Hvor enig eller uenig er du i at trafikkdata bidro med informasjon av stor betydning for etterforskningen i denne saken

Alternativer	Prosent	Verdi
1 Helt uenig	4,8 %	3
2 Litt uenig	11,1 %	7
3 Verken uenig eller enig	11,1 %	7
4 Litt enig	30,2 %	19
5 Helt enig	42,9 %	27
Total		63

Gjennomsnitt		3,95
Standard avvik		1,19
Median		4,0

4. Dersom trafikkdata hadde betydning for etterforskningen i denne saken, hvilke opplysninger bidro det med? (flere svar mulig)

Alternativer	Prosent	Verdi
1 Identifisering av gjerningsperson(er)	19,6 %	9
2 Kontroll av mistenkte/siktedes bevegelser	34,8 %	16
3 Kontroll av opplysninger fremkommet i politiavhør eller andre undersøkelser	73,9 %	34
4 Kartlegge personer i et bestemt område (basestasjonsutskrifter)	4,3 %	2
5 Sjekke personer inn/ut av saken	34,8 %	16
6 Opplysninger om mistenktes/siktedes kontaktmønster (kontaktanalyse)	54,3 %	25

7	Trafikkdata var ressursbesparende for saken ved at andre metoder/undersøkelser kunne utelates	13,0 %	6
8	Annet:	8,7 %	4
Total			46

Gjennomsnitt	4,06
Standard avvik	1,92
Median	3,0

5. Hvorfor ble det ikke innhentet trafikkdata i denne saken?

Alternativer		Prosent	Verdi
1	Det ble ikke vurdert	27,7 %	43
2	Det ble vurdert, men det var ikke nødvendig for etterforskningen	61,3 %	95
3	Det ble vurdert som nødvendig, men det var for kostbart	0,0 %	0
4	Det ble vurdert som nødvendig, men data var slettet pga kort lagringstid	5,8 %	9
5	Annet	5,2 %	8
Total			155

Gjennomsnitt	1,99
Standard avvik	0,99
Median	2,0

6. Hvor enig eller uenig er du i at det ville vært relevant å innhente historiske trafikkdata lengre tilbake i tid i denne aktuelle saken med hensyn til:

I dag lagres historiske trafikkdata hos teleselskapene i henholdsvis 150 dager hos Netcom og i 90 dager hos Telenor. IP-trafikk kan lagres i 21 dager.Hvor enig eller uenig er du i at det ville vært relevant å innhente historiske trafikkdata lengre tilbake i tid i denne saken med hensyn til:

Alternativer		N
1	Trafikkdata fra mobil-/fasttelefoni	215
2	IP-trafikk	203

6.1 Hvor enig eller uenig er du i at det ville vært relevant å innhente historiske trafikkdata lengre tilbake i tid i denne aktuelle saken med hensyn til: - Trafikkdata fra mobil-/fasttelefoni

Alternativer		Prosent	Verdi
1	Helt uenig	37,2 %	80
2	Litt uenig	4,7 %	10
3	Verken uenig eller enig	13,5 %	29
4	Litt enig	7,9 %	17
5	Helt enig	36,7 %	79
Total			215

Gjennomsnitt	3,02
Standard avvik	1,76
Median	3,0

6.2 Hvor enig eller uenig er du i at det ville vært relevant å innhente historiske trafikkdata lengre tilbake i tid i denne aktuelle saken med hensyn til: - IP-trafikk

Alternativer	Prosent	Verdi
1 Helt uenig	37,4 %	76
2 Litt uenig	5,4 %	11
3 Verken uenig eller enig	18,2 %	37
4 Litt enig	3,0 %	6
5 Helt enig	36,0 %	73
Total		203

Gjennomsnitt		2,95
Standard avvik		1,74
Median		3,0

POLITIET

Forbnyings- og administrasjonsdepartementet
Boks 8004, Dep
0030 OSLO

Deres referanse	*Vår referanse*	*Dato*
200900158	200900415 -2	18.08.2009

Høring - NOU 2009:1 Individ og Integritet

Det vises til horingsbrev av 17.12.09 om NOU 2009:1 Individ og integritet.

Personervernkommisjonens utredning reiser omfattende og vanskelige spørsmål og avveiinger. Kripos høringssuttalelse konsentrerer seg om de vurderinger vi mener vil kunne få direkte betydning for politiets mulighet for å gjennomføre etterforsking og for ovrig ivareta politiets ansvarsområde. Vi har i liten grad gått inn i de spørsmål som gjelder personvern i arbeidslivet, helsevesenet mv, selv om dette er viktige spørsmål og også – i det minste indirekte – vil ha betydning for politiets etterforskingsmuligheter.

1. Avveining mellom personvern og andre hensyn
Kommisjonens mandat var blant annet å vurdere nærmere hvordan personvernet bor tas vare på i møtet med motstridende hensyn og verdier. Slike interesseavveininger synes i mindre grad å være fulgt opp av kommisjonen. I hovedsak er det utfordringene for personvernet som beskrives.

I utredningens pkt 7.5 fastslås at "*personvern er en menneskerettighet som ikke kan relativiseres*." Kripos er ikke enig i dette. Personvern må anses som en grunnleggende menneskerettighet, men den må relativiseres når det oppstår konflikt i forhold til andre grunnleggende menneskerettigheter, eller andre personers personvern. Teknologiske og juridiske tiltak som isolert sett kan være personvernfremmende for enkelte, slik som f.eks anonymisering og sletting av opplysninger, kan i praksis resultere i svært alvorlige personvernkrenkelser for andre. Kripos vil her særlig vise til at EMKs artikkel 8 implisitt pålegger staten et ansvar for å sikre at man kan forebygge, avverge og forfølge krenkelser. Vi viser her til EMD's dom av 2. desember 2008 (sak 2873/02) som omtales nærmere nedenfor.

En kan ikke se at kommisjonen har foretatt noen prinsipiell drøftelse av om tiltak som i noen sammenhenger kan styrke personvernet, også kan bidra til å svekke personvernet i andre sammenhenger. I rapporten, eksempelvis kapittel 9 (Teknologiske trender som utfordrer personvernet) beskrives utfordringene for personvernet hovedsakelig som ny teknologi som store systemeiere står bak. Kapittel 10 og vedlegg 4 beskriver "Personvernfremmende teknologier", dvs anonymisering, kryptering etc. En av dagens storste utfordringer for personvernet er aktiviteter fra kriminelle. Nettbankbedragerier, datainnbrudd, trusler og sjikane via internett, spredning av overgrepsbilder etc, er eksempler på aktiviteter som ved bruk av anonymiserende tjenester og pålagt sletting av elektroniske spor blir lettere å gjennomfore og vanskeligere å avdekke og stanse. Det er en gjennomgående mangel ved rapporten at denne typen utfordringer for personvernet ikke

Kripos
Den nasjonale enhet for bekjempelse av organisert og annen alvorlig kriminalitet
Brynsalléen 6, Postboks 8163 Dep, 0034 OSLO
Tlf: 23 20 80 00 Faks: 23 20 88 80
E-post: kripos@politiet.no Org.nr.: 974 760 827

beskrives, ettersom mulige løsninger for denne type uønsket aktivitet kan være annerledes enn mulige løsninger mot eventuelle krenkelser foretatt av store systemeiere.

Rapporten etterlater derfor et ubalansert helhetsinntrykk av at anonymisering, manglende brukerregistrering og sletting av elektroniske spor pr. definisjon styrker personvernet. Kripos er av den oppfatning at anonymisering, manglende brukerregistrering og sletting av elektroniske spor er nøytrale tiltak, som i noen sammenhenger kan styrke personvernet for den enkelte og i andre sammenhenger krenke personvernet.

2. Lagring av trafikkdata

Personvernkommisjonen synes å legge til grunn at det ikke er dokumentert at lagrede trafikkdata har særlig betydning for politiets arbeid, og kommisjonens rapport fokuserer på motforestillingene mot lagring, uten å foreta en interesseavveiing hvor også behovene for tilgang til denne type bevis beskrives. Kripos benytter jevnlig lagrede trafikkdata i etterforsking av alvorlig kriminalitet, og ofte er tilgang på trafikkdata avgjørende for oppklaring. Det er ikke vanskelig å dokumenterte at lagring av trafikkdata vil ha betydning for politiets etterforsking, men dette må selvsagt avveies mot det inngrep i personvernet dette representerer. Kripos vil i det følgende gi en kortfattet beskrivelse av nåværende bruk og behov for slike data. Vi antar imidlertid at en nærmere diskusjon om hvilke data som bør lagres hvor lenge forutsetter en grundigere vurdering og at dette formodentlig kan skje i forbindelse med en høring om implementering av EU's datalagringsdirektiv, eventuelt en vurdering av å innføre nasjonale regler om lagring.

Betydning for politiets arbeid

Telefoni, internett og øvrige former for elektronisk kommunikasjon medfører elektroniske bevis som kan ha betydning for politiets arbeid i ulike sammenhenger. I likhet med andre typer bevis som kan føres for domstolene, innebærer prinsippene om fri bevisførsel og fri bevisvurdering at domstolene skal foreta en konkret vurdering av alle tilgjengelige beviser som framlegges. I tråd med norsk rettstradisjon mener Kripos at regelverket omkring personvern i størst mulig grad må være innrettet slik at det er mest mulig teknologinøytralt, at det foretas en rettspolitisk avveiing av de mulige kryssende interesser og at det tas utgangspunkt i det alminnelige prinsipp om fri bevisførsel og fri bevisvurdering. Kripos har erfart at selv om en del kriminelle miljøer forsøker å unngå inkriminerende elektroniske spor, er det mulig å innhente relevante elektroniske spor også i slike saker. Selv profesjonelle kriminelle alltid klarer ikke alltid å skjule sine spor, - enten dette gjelder elektroniske spor, fingeravtrykk eller DNA-spor.

Det er ikke mulig å sette opp en uttømmende oversikt over hvilken potensiell betydning ulike typer elektroniske bevis kan ha i politiets arbeid. Ulike typer trafikkdata har vært benyttet og blir benyttet i et vidt spekter av saker, eksempelvis:

- drapssaker og savnede personer
- nettverksetterforskning: narkotikasaker, menneskesmugling, ransmiljøer og øvrig organisert kriminaliet
- seriesaker
- samarbeid med utlandet
- distribusjon av barnepornografi og spredning av overgrepsbilder
- datakriminalitet: nettbank-bedragerier, datainnbrudd, tjenestenektangrep etc
- trusler mot skoler via nettsamfunn som YouTube, Facebook etc

Kommisjonen drøfter ikke i hvilken grad manglende oppklaring av denne type saker er et akseptert resultat av sletting av trafikkdata som kommisjonen synes å gå inn for. Kripos forutsetter at dette underlegges en grundig vurdering når datalagringsdirektivet skal behandles.

Kripos finner i denne sammenheng grunn til å stille spørsmål ved holdbarheten av noe av grunnlagsmaterialet kommisjonens uttalelse om datalagringsdirektivet bygger på (Vedlegg 1: Uttalelse om datalagringsdirektivet, fotnote 2). I den grad slike dokumenter skal vektlegges i prosessen rundt datalagringsdirektivet, må det kunne forventes at de gjennomgås nøye mht kvalitet og holdbarhet. Vedlagt følger et problemnotat med nærmere beskrivelse av forholdene.

Kripos er uansett uenig i synspunktet om at oppklaringsprosent er det viktigste målepunktet for å belyse politiets behov for trafikkdata. Utfallet av en straffesak er sjelden avhengig av ett eneste bevis. Et eksempel: Baneheia-saken, hvor bl.a. ulike trafikkdata for mobiltelefoner, en DNA-analyse, vitneforklaringer og forklaring fra en medtiltalt samlet bidro til domfellelse. Flere og bedre bevis gir bedre kvalitet på politiets etterforskning og kan gi raskere saksbehandling. Trafikkdata kan også bidra til å eliminere uskyldige. Det bør dessuten synliggjøres at lengre lagring av denne informasjonen hos teleselskapene vil kunne medføre at eventuelle inngrep i publikums privatliv kan bli avdempet. Årsaken er at gitt bedre tid, vil politiets innhenting av trafikkdata kunne være mer målrettet enn i dag. Når lagringstiden er kort vil politiet på grunn av faren for at informasjonen går tapt måtte hente inn trafikkdata om flere aktuelle personer, mot for å vente til man har silt tilgjengelig informasjon bedre. Dette medfører også større kostnader og betydelig merarbeid for politiet, noe som igjen senker farten på etterforskningen.

Vi vil også fremheve at betydningen av tilgang til trafikkdata kan ha betydning langt ut over den aktuelle straffesak. Et eksempel her er den senere tids utvikling med trussler mot skoler og alvorlige trussler fremsatt på internett, hvor det er av avgjørende betydning raskets mulig å få et best mulig grunnlag for å avgjøre om man kan anta at faren ikke er reell eller om det må iverksettes omfattende sikringstiltak som både er kostbare og svært belastende for de det gjelder.

Lagringstid

I rapportens pkt 17.4.2 beskrives datalagringsdirektivet og relaterte spørsmål. På s 190 framgår at en del trafikkopplysninger for internett lagres i 3-5 måneder. Dette er ikke lenger à jour grunnet Datatilsynets avgjørelse fra mai 2009, hvor tilsynet legger til grunn at trafikkdata nå skal slettes etter maksimalt 21 dager. Avgjørelsen reiser etter Kripos syn flere spørsmål, både i forhold til personvernmyndighetenes rolle (se nærmere under pkt 4) og også i forhold til det rettslige rammeverket (personopplysningsloven, ekomloven, og den antatt kommende prosessen for datalagringsdirektivet).

"Frysing" av data

Det blir undertiden hevdet at "frysing" av data er et tilstrekkelig alternativ til lagring. Strpl. §215a gir hjemmel for sikringspålegg, hvor eksempelvis en ISP pålegges å "fryse" relevante trafikkdata inntil videre. Problemet er at politiet før et slikt pålegg kan gis, både må ha kunnskap om at et straffbart forhold har funnet sted, lete etter elektroniske bevis, og knytte disse til en bestemt ISP innen slettingen har skjedd. Det er ikke alltid mulig. I mange tilfeller er det også behov for å undersøke flere ledd med informasjon, eksempelvis etterforskning

av seriesaker. Da vil ofte nødvendige bevis for å identifisere mistenkte være lengre tilbake i tid. Kripos anser at sikringspålegg er et virkemiddel som har betydning i mange tilfeller, men som ikke kan erstatte lagring av trafikkdata. Det må understrekes at tidsaspektet her er blitt ytterligere forsterket etter Datatilsynets avgjørelse nevnt ovenfor om maksimalt 21 dagers lagringstid.

Jurisdiksjon

Jurisdiksjon er en særlig utfordring. Ifølge Interpol har 8 av 10 tilfeller av datakriminalitet spor til andre land. Dagens situasjon i Norge er en generell sletteplikt og en kort datalagringstid: mellom null og 21 dager. Dette er motsatt retning av hva som skjer for de landene som har innført datalagringsdirektivet. Ikke-innføring av Datalagringsdirektivet i Norge vil ikke påvirke hvordan f.eks. utenlandske e-postleverandører lagrer data tilknyttet norske brukere, men vil gjøre det vanskeligere for politi og domstoler i andre land å innhente elektroniske spor som fører til Norge. Norsk politi kan fortsatt få tilgang til data lagret i andre land (jf. Rt. 2002/1744, telefonavlytting fra Spania benyttet i Norge), men tilknyttede norske IP-adressene kan være "kalde spor" etter få dager.

Kripos er politiets kontaktpunkt mot utlandet, vi mottar rettsanmodninger og etterretningsinformasjon fra resten av verden og etterkommer dette i tråd med Norges internasjonale forpliktelser. Av de vanligste henvendelsene Kripos mottar, er ønsket om trafikkdata fra telefonnummer i norsk nett. Det er en realitet at internasjonal korrespondanse tar tid, bare saksbehandlingsreglene for rettsanmodninger medfører et byråkrati hvor alle ledd fra etterforsker til justisdepartement involveres hos både anmodende og anmodede stat. Dagens lagringstid medfører derfor at Norge i mange tilfeller ikke kan bistå våre internasjonale samarbeidspartnere med det de ber om.

Det er også vanlig at etterforskning i utlandet avdekker mulige gjerningspersoner eller straffbare forhold i Norge. Dette er informasjon som ofte ikke tilflyter oss før etterforskningen er godt i gang eller sågar ferdigstilt i opphavslandet. Dette kan gjelde narkotikasmuglere, menneskehandlere eller ranere, men det er kanskje mest tydelig ved bekjempelse av overgrep mot barn på internett. Her har vi en rekke eksempler på at nordmenn som har deltatt i spredningen av overgrepsbilder av barn på internett ikke blir avslørt fordi informasjonen om datatrafikken ikke er lagret lenge nok.

I enkelte sammenhenger har Personvernkommisjonen etterlyst mer innsats fra politiet, for eksempel i forhold til barn og nettbruk, jf. utredningens kapittel 14. I Datatilsynets høringsuttalelse til Faremo-rapporten (avgitt 7.5.2007) blir det spesifikt bedt om mer innsats fra Kripos. Temaet for rapporten var forebygging av internettrelaterte overgrep mot barn. En utvidet sletteplikt vil ikke bedre Kripos sine arbeidsmuligheter på dette saksområdet.

Forhold til EMK

EMD behandlet nylig saken K.U. v. Finland: dom fra EMD av 2.12.2008 (sak 2873/02), hvor temaet var EMK art. 8 i forhold til ikke-lagring av abonnent- og trafikkdata.

En 12 år gammel gutt hadde blitt seksuelt sjikanert via Internett. Hans far ba politiet etterforske saken, men saken stoppet opp pga. ISPens taushetsplikt. Denne taushetsplikten var i strid med EMK art. 8, og Finland ble dømt til å betale erstatning.

En av nøkkelvurderingene omkring interesseavveiing mellom kriminalitetsbekjempelse og personvern framkommer i avgjørelsen pkt. 49:

"An effective investigation could never be launched because of an overriding requirement of confidentiality. Although freedom of expression and confidentiality of communications are primary considerations and users of telecommunications and Internet services must have a guarantee that their own privacy and freedom of expression will be respected, such guarantee cannot be absolute and must yield on occasion to other legitimate imperatives, such as the prevention of disorder or crime or the protection of the rights and freedoms of others."

EMD-avgjørelsen K.U. vs Finland pålegger medlemsstatene et ansvar for at krenkelser av privatpersoner etter EMK art. 8 skal kunne håndheves. Hvis det nasjonale lovverket svikter, vil vedkommende stat kunne bli dømt for brudd på menneskerettighetene og tilpliktet å betale erstatning.

Kopi av avgjørelsen følger vedlagt.

3. Nettnemnd

Kripos slutter seg til Personvernkommisjonens forslag om å etablere et organ som kan bidra til å utvikle gode etiske retningslinjer for nettytringer og løse konflikter om publisering på nettet.

Kripos mottar en del henvendelser vedrørende nettkrenkelser som ikke er straffbare forhold eller som ligger i gråsonen av hva som er straffbart. Saker som omhandler bilder som blir lagt ut på nettet hvor vedkommende angrer i ettertid på publiseringen, ærekrenkelser som ikke kan følges opp strafferettslig, bilder som blir lagt ut på nettet og som misbrukes i andre sammenhenger er eksempler på saker som ofte ikke blir prioritert av politiet. Det oppleves ikke tilfredsstillende å måtte henvise publikum, særlig barn og unge, til internettleverandører eller til sivile søksmål for å få løst konflikter om publisering på nettet som oppleves som krenkende.

Etter vår erfaring vil det være formålstjenelig med et offentlig organ som vil være et lavterskeltilbud hvor konflikter om nettytringer kan løses utenfor rettsapparatet, særlig i konflikter hvor barn og unge er involvert. Det er prinsipielt viktig at dette organet skal være basert på frivillighet mellom partene, at organet i hovedsak vil ha en rådgivende funksjon og at når man ikke kommer til enighet, løses konflikten ved en eventuell domstolsbehandling.

Personvernkommisjonen mener nemda bør ha et bredt virkeområde og i utgangspunktet kunne dekke de fleste typer av krenkelser på nettet. Hvilke saker som skal ligge under nemda sitt ansvarsområde, saksbehandlingsregler, forholdet til utenlandske virksomheter og praktiske muligheter for bevissikring (IP-adresse) er forhold som bør vurderes nærmere av en arbeidsgruppe som følger opp dette arbeidet i ettertid.

4. Organisering av personvernmyndighetene.

Kripos slutter seg til Personvernkommisjonens generelle vurderinger i kapittel 18 om Datatilsynets rolle som henholdsvis ombud og tilsynsmyndighet.

Datatilsynet har en aktiv mediastrategi og er en tydelig samfunnsdebattant for å fremme personvernhensyn og skape bevissthet og debatt om personvernspørsmål. Fra Datatilsynets årsmelding heter det at *"Aktiv kommunikasjonsvirksomhet er dermed et virkemiddel som vektlegges sterkt"*. En slik påvirker-rolle kan komme i konflikt med rollen som myndighetsutøver etter personopplysningsloven.

Avgjørelser etter personopplysningsloven bygger i stor grad på utpregede skjønnsmessige vurderinger. Sentrale bestemmelser i lovverket har vurderingsnormer som "saklig begrunnet", "tilstrekkelig", "tilfredsstillende", "nødvendig", mv. Et tydeliggjort standpunkt i forkant, f.eks gjennom media, der man på bakgrunn av ombudsrollen har lagt særlig vekt på personvernhensynene, kan gjøre det vanskeligere å foreta en objektiv interesseavveining i etterkant. Satt på spissen kan det i slike tilfeller oppstå inhabilitetslignende spørsmål. Uavhengig av hvordan tilsynet behandler saken, er det grunn til å spørre om denne organiseringen svekker publikums og berørte parters tillit til Datatilsynet.

Til illustrasjon vises til Datatilsynets vedtak fra mai 2009 nevnt ovenfor, hvor tilsynet i egenskap å være myndighetsutøver vedtok en maksimal lagringstid på 3 uker for to større ISPer. På bakgrunn av Datatilsynets engasjement som sterk motstander av å implementere datalagringsdirektivet, noe som klart faller inn under ombudsrollen, kan det stilles spørsmål ved i hvilken grad vedtaket om lagringstid bærer preg av dette standpunktet.

Dette har særlig betydning for spørsmål som krever brede samfunnsmessige vurderinger, eksempelvis innen helse- eller justissektoren, eller andre tilfeller hvor personvernhensyn må veies mot andre interesser. Det vises i denne sammenheng til utkast til politiregisterlov hvor Datatilsynet skal være tilsynsmyndighet. Tilsynets påleggskompetanse foreslås her innskrenket i spørsmål av utpreget politifaglig art. I slike tilfeller vil tilsynets rolle være å påse at en vurdering er foretatt, ikke å overprøve innholdet i vurderingene.

Det kan derfor synes hensiktsmessig å etablere et klarere skille mellom Datatilsynets rolle som ombud og rollen som myndighetsutøver, jf. forslaget fra et mindretall i Personvernkommisjonen om å omgjøre Datatilsynet til et Personverntilsyn underlagt Justisdepartementet, og samtidig opprette et uavhengig personombud oppnevnt av Stortinget, jf. NOU 2009:1 side 207.

5. Grunnlovsfesting

Avslutningsvis vil Kripos kort kommentere forslaget om grunnlovfesting av personvernet. Kripos er i utganspunktet ikke i mot en grunnlovsfesting, men synes det er vanskelig å ta stilling til hensiktsmessigheten av spørsmålet så lenge det ikke finnes noen entydig definisjon av personvern, og så lenge man ikke har konkretisert ordlyden i en eventuell Grunnlovsbestemmelse. En forutsetning for grunnlovsvern bør være en klarere definisjon og en avklaring av om bestemmelsen skal utformes som en skranke for den alminnelige lovgivning.

Med hilsen

Odd Olsen Ingerø

Ketil Haukaas

Kopi: Politidirektoratet

Vedlegg
- EMD-avgjørelse K.U. vs. Finland, 2.12.2008
- Notat vedrørende vedlegg 1 til NOU 2009: