POLITIET

Fornyings-, administrasjons- og kirkedepartementet
Postboks 8004 Dep.
0030 OSLO

postmottak@fad.dep.no

Deres referanse	*Vår referanse*	*Dato*
12/2016	2012/00701-3	28.9.2012

Høringsuttalelse – Forslag til endringer i personopplysningsforskriften

Kripos viser til høringsbrev fra Fornyings- administrasjons- og kirkedepartementet av 26. juni 2012 vedrørende forslag til endringer i personopplysningsforskriften. Høringsfrist er satt til 1. oktober i år.

Innledningsvis ønsker Kripos å påpeke at del A i høringsforslaget er del av et omfattende og krevende arbeid med implementering av datalagringsdirektivet. Flere myndigheter og virksomheter har vært, og er, involvert i prosesser rundt utarbeidelse av regelverk og kontroll- og tilsynsmekanismer, samt fordeling av kostnader. Kripos har deltatt aktivt i implementeringsprosessene og er fremdeles tungt engasjert i deler av det arbeidet som pågår.

Flere av prosessene både påvirker og er avhengig av hverandre. Kripos og andre involverte aktører har derfor etterlyst en mer helhetlig behandling av de ulike elementene ved implementeringen. Det er en forutsetning for god implementering at man i tilstrekkelig grad avklarer prosessenes betydning for hverandre og undergir dem en nødvendig felles behandling.

Merknader til de enkelte forslagene følger under.

Del A – data som faller inn under lagringsplikten i datalagringsdirektivet

Datatilsynet sendte den 29. mars i år utkast til "konsesjon til å lagre personopplysninger i medhold av ekomloven § 2-7a" på høring. Kripos hadde en rekke innspill til utkastet av sentral betydning for politiet, men kan ikke se at noen av disse er ihensyntatt i den versjon av standardkonsesjon som nå foreligger.

For Kripos fremstår det som uheldig og lite hensiktsmessig at endringer i personopplysningsforskriften § 7-1 sendes på høring i etterkant av at Datatilsynet har fastsatt endelig konsesjonstekst på området. Etter vår oppfatning er det nødvendig at den endelige konsesjonsteksten gjennomgås på ny, sett i lys av datalagringsforskriften, samt

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

en eventuell vedtakelse av den foreslåtte § 7-1 i personopplysningsforskriften og elementer som måtte fremkomme i denne høringsrunden.

Kripos vil påpeke særlig to sentrale punkter som det bør tas høyde for i forbindelse med den foreslåtte endringen i personopplysningsforskriften § 7-1. I det øvrige, og for mer utfyllende merknader, vises det til våre høringsuttalelser avgitt i forbindelse med datalagringsforskriften og utkast til konsesjon fra Datatilsynet. Høringssvarene følger vedlagt dette brev.

- *Type opplysninger - hashing*
  Etter Kripos' vurdering bør det i framgå av forskriftsforslaget at det i konsesjon fra Datatilsynet klargjøres hvilke verdier/opplysninger som skal hashes og som således kan innhentes fra politiet i henhold til formålet med datalagringsdirektivet. Hvilke verdier som er søkbare er helt avgjørende for politiets nytteverdi av opplysningene.

- *Overføringsmetode*
  For politiet er det avgjørende at det etableres en ensartet overføringsmetode av data mellom lagringspliktig og politi. Det er etter vår oppfatning av stor betydning at man får etablert et felles lagringsformat, jf. tilretteleggingsplikten i datalagringsforskriften § 4-3. Et felles lagringsformat er nødvendig for å ivareta sentrale elementer i prosessen, som tilgjengelighet, ensartethet og kvalitet på opplysningene.

Del B – kameraovervåking

Så vidt Kripos forstår forslaget til endringer i personopplysningsforskriftens kapittel 8, er disse i hovedsak av kosmetisk karakter for å tilpasse forskriften til allerede gjennomførte endringer i personopplysningslovens kapittel VII om kameraovervåking. Kripos har ingen merknader til dette.

Når det gjelder politiets bruk av opptak og den foreslåtte endringen av forskriftens § 8-3, ser Kripos at det av pedagogiske hensyn kan være hensiktsmessig å samle reguleringen av politiets bruk av billedopptak i en bestemmelse. I så måte bør det vurderes om forskriftens § 8-4 fjerde ledd bokstav a og femte ledd bør flyttes til den foreslåtte § 8-3.

Kripos legger videre til grunn at den foreslåtte bestemmelsen i § 8-3 annet ledd ikke er ment å gjøre endringer i dagens rettstilstand for innsyn i billedopptak som politiet er i besittelse av, slik at det fortsatt vil være straffeprosesslovens bestemmelser som regulerer om den enkelte kan gis innsyn i billedmaterialet eller ikke.

Med hilsen

Ketil Haukaas

Saksbehandler:
seniorrådgiver Christine Ask Ottesen
tlf 23208227

Kopi til:
Riksadvokaten
Det nasjonale statsadvokatembetet
Politidirektoratet

Vedlegg:
Kripos' høringssvar av 10. april 2012
Kripos' høringssvar av 19. april 2012

VEDLEGG

POLITIET

Post- og teletilsynet
Postboks 93
4791 LILLESAND

Sendt elektronisk til firmapost@npt.no

Deres referanse	*Vår referanse*	*Dato*
1102068-22 – 417.1	201200206	10. april 2012

DATALAGRINGSFORSKRIFTEN – HØRINGSSVAR FRA KRIPOS

1. INNLEDNING

Det vises til Post- og teletilsynets høringsbrev av 7. februar 2012 med vedlagt utkast til forskrift om lagringsplikt for bestemte data og om tilrettelegging av disse (datalagringsforskriften). Frist for kommentarer til utkastet er satt til 10. april 2012.

Som tilsynet er kjent med har Kripos deltatt i den prosess som har ledet frem til utkastet, og har – så langt som mulig – søkt å fremme klare og tydelige meninger innenfor de områder som har vært på agendaen. De vises særlig til de "stormøter" som har vært avholdt i tilsynets regi, henholdsvis den 10. august, 29. september og 3. november 2011, og til vårt skriftlige innspill i prosessen gjennom notat av 16. desember 2012.

Implementering av DLD er en krevende prosess. Som tilsynet selv påpeker er flere departementer, tilsyn og andre myndigheter involvert i utarbeidelsen av nødvendig regelverk og andre former for kontroll- og tilsynsmekanismer. Samtidig skal kostnader ved implementeringen fordeles, nye tekniske systemer etableres/tilpasses og det skal avklares hvordan man praktisk skal gå frem i relasjonen mellom de som skal lagre data og de som har krav på å få data utlevert. Flere av disse prosessene påvirker, og er avhengige av, hverandre. Eksempelvis vil krav til sikkerhet påvirke kostnader, som vil påvirke modell for kostnadsfordeling, som vil påvirke grensen for hvem som skal lagre og krav til tilrettelegging, som vil være avgjørende for hva politiet kan forvente å få, som igjen blir avgjørende for om lagringen faktisk vil tjene sitt formål, nemlig å være et verktøy til bruk for etterforskning, oppklaring og straffeforfølgning av alvorlige straffbare forhold.

Kripos har opplevd omfanget og de parallelle prosessene som utfordrende. Det har fra Kripos – og fra andre – vært etterlyst en mer samlet behandling av de forskjellige elementer ved implementeringen. Denne utfordringen står fortsatt ved lag. Kripos mener det er en forutsetning for en god implementering at man i fortsettelsen i tilstrekkelig grad

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

avklarer prosessenes betydning for hverandre og undergir dem en nødvendig felles behandling.

Tilsynets forskriftsarbeid er en sentral del av implementeringen og berører temaer som er viktige for politiet. Som sagt har Kripos tidligere levert skriftlig innspill på områder som fremstår som særlig sentrale. Hoveddelen av disse står fremdeles ved lag og fremmes nå i den formelle høringsprosessen som del av vårt høringssvar. Dette gjelder temaene hvem skal lagre (kap 3), hva skal lagres (kap 4) og tilrettelegging/uthenting (kap 5). Våre synspunkter har sitt grunnleggende utgangspunkt i formålet med den lagring som er bestemt implementert (kap 2).

Særlige kommentarer til enkeltpunkter i tilsynets utkast er inntatt dels under kapitlene over og dels under kap 6. Under kap 6 følger også noen særlige kommentarer til selve forskriftsteksten.

2. FORMÅLET MED LAGRINGEN

Data har til nå vært lagret frivillig. Formålet har vært selskapenes egen administrasjon – blant annet fakturering av kunder. Ved implementering av direktivet endres dette utgangspunkt radikalt. Gjennom ny ekoml § 2-7a får selskapene nå en plikt til lagring og formålet med lagringen er ene og alene politiets behov for dataene som verktøy i sin etterforskning. Sammen med lagringsplikten følger (som før) en plikt til tilrettelegging for tilgang (gjeldende ekoml § 2-8).

Når formålet med implementeringen, plikten til lagring og tilrettelegging av data er å tjene som verktøy *"....til bruk for etterforskning, oppklaring og straffeforfølging ....."*, er det avgjørende at dette også vektlegges i tilstrekkelig grad ved utforming av forskriftene. Disse vil på mange områder vil bli helt avgjørende for politiets mulighet til i praksis å nyttiggjøre seg data som et reelt etterforskningsverktøy.

Kripos mener tilsynet i for liten grad har vektlagt dette formålet i den vekting av hensyn som følger av utkastet. Det vises særlig til kretsen av lagringspliktige subjekter og responstid. Etterforskning, oppklaring og straffeforfølgning av alvorlige straffbare forhold er politi- og påtalemyndighets fagfelt. Vi står nærmest til å vurdere hva som kreves for at lagringen skal bli det verktøy for kriminalitetsbekjempelse som er forutsatt ved implementeringen. De signaler som er gitt fra Kripos i prosessen er etter vår mening ikke vektlagt i tilstrekkelig grad av tilsynet, og vi mener dette kan få alvorlige konsekvenser for vår evne til effektiv kriminalitetsbekjempelse. Forholdene vil bli kommentert nærmere nedenfor under kap 3 - 5.

3. HVEM SKAL LAGRE

Det er dataene som genereres / behandles (trafikkdata, lokaliseringsdata og identifiseringsdata) som er viktige for politiet. Hvor de lagres og hvem som er behandlingspliktig er som et utgangspunkt uten særlig betydning så lenge data lagres og er tilgjengelige for utlevering ved behov. Skal en lagring oppnå sitt formål fullt og helt

vil konsekvensen være at alt som genereres / behandles av denne type data må lagres. Følger man dette utgangspunktet videre har det blant annet den følge;

- at også subjekter som genererer / behandler denne type data - men som pr i dag ikke omfattes av definisjonen av lagringspliktige etter ekomloven (*"...tilbyder av elektronisk kommunikasjonsnett som anvendes til offentlig elektronisk kommunikasjonstjeneste og tilbyder av slik tjeneste....")* - må pålegges en plikt til å lagre gjennom forskriften (eventuelt ved enkeltvedtak), og at
- dersom man skal unnta særlige subjekter på grunn av størrelse eller andre forhold må det skje under den forutsetning at aktuelle data likevel lagres (av andre/andre steder).

Kripos ser at et slikt utgangspunkt på enkelte områder kan få følger som ikke står i forhold til den forventede effekt av lagringen som etterforskningsverktøy. Det må likevel foretas en konkret vurdering av omfanget, med ovenstående som utgangspunkt. Slik Kripos oppfatter dagens situasjon kan det ved denne vurdering være naturlig å dele de aktuelle lagringspliktige inn i tre hovedkategorier, henholdsvis:

1. Teleselskaper / ISP-er.
2. Andre som tilbyr internettaksess (eks hoteller, universiteter, store bedrifter osv).
3. Tilbyder av tjenester på applikasjonsnivå (eks Opera, "rene" epostleverandører osv).

1. Teleselskaper / ISP-er

Slik Kripos oppfatter tilsynets utkast vil alle subjekter som inngår i kategori 1 omfattes av lagringsplikten.

Kripos' klare vurdering er at ingen norske teleselskaper/ISP-er kan unntas fra lagringsplikten, så lenge de tilbyr offentlig tilgjengelige tjenester i det norske marked. Det må være forutsigbart hvem som faller inn under denne kategorien, både av hensyn til politiets og tilbydernes behov. Gjør man unntak fra dette utgangspunktet vil det uthule formålet med lagringsplikten. Spørsmålet er heller i hvilken grad forskriften skal utvides til å gjelde andre aktører enn de som inngår i kategori 1.

2. Andre som tilbyr internettaksess

Tilsynets definisjon av internettaksess (pkt 4.3.5) avgrenser ikke mot såkalte private nett, men det blir avgresningen av gruppen lagringspliktige subjekter som vil avgjøre om data fra private nett skal lagres.

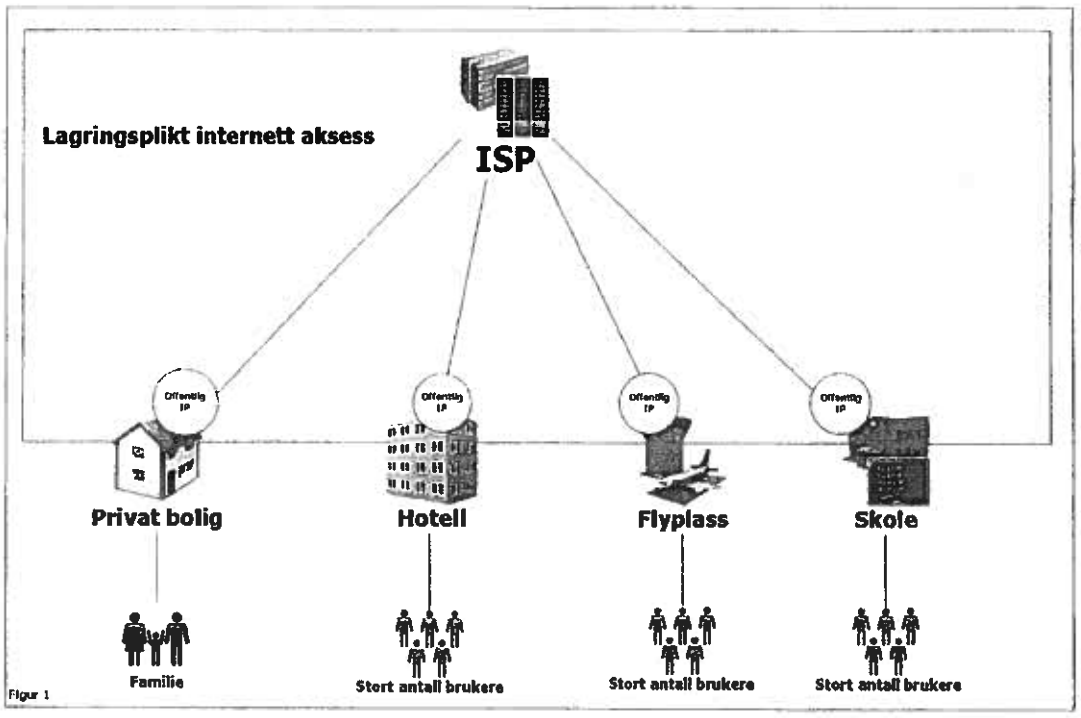
Tilsynet foreslår som nevnt at det er tilbyderbegrepet i ekomloven som er utgangspunktet for hvem som skal underlegges lagringsplikt, uavhengig av datatype. For internettaksess vil dette etter Kripos' syn bety at formålet med lagringen ikke kan oppfylles. Tilsynets foreslåtte løsning vil pålegge lagringspliktige ISP-er å lagre hvilke IP-adresser de har tildelt sine kunder de siste 6 måneder. Det er altså kun kundens offentlige IP-adresse som skal lagres, se fig 1.

For private boliger betyr dette at man får opplysinger om hvilken ip-adresse kunden, dvs boligen, har benyttet til en hver tid, men ikke nødvendigvis hvem i husstanden, eventuelt i husstandens umiddelbare nærhet, som har benyttet internett på det konkrete tidspunkt.

Her vil det være en begrenset personkrets som er aktuelle. Hvem som var den konkrete bruker kan politiet finne ut gjennom ransaking/beslag og datatekniske undersøkelser etter de ordinære reglene om dette i straffeprosessloven.

Sett fra et etterforskningsmessig synspunkt oppstår det langt større problemer dersom ip-adressen politiet ønsker å spore går til en abonnent/kunde som tilbyr internettaksess eksternt, eksempelvis et hotell. Den foreslåtte løsning medfører at politiets spor stopper ved den tildelte offentlige ip-adresse, mens det kan finnes et meget betydelig antall brukere som har benyttet samme offentlige ip-adresse, eksempelvis alle reisende på Oslo lufthavn Gardermoen eller alle beboere på Radisson Plaza hotell. Andre eksempler er store trådløse nett som eksempelvis Uninett[1], Trådløse Trondheim[2] eller Drammen kommunes tilbud om trådløse soner[3].

Resultatet av den foreslåtte løsning er at politiet, gjennom de lagringspliktige dataene hos ISP, vil finne ut at den aktuelle brukeren har koblet seg til via eksempelvis hotellets løsning for internettaksess (hotellets offentlige ip-adresse). Dersom hotellet ikke pålegges lagringsplikt for tildelte ip-adresser i sitt nett, vil man ikke ha noen mulighet for å finne frem til hvem som var den reelle brukeren av den aktuelle ip-adressen. Formålet med lagringen kan derfor ikke oppfylles.



Lagringsdata knyttet til internettaksess er begrenset til hvem som bruker de aktuelle ip-adressene på gitte tidspunkt. Dataene er kun egnet til å identifisere brukeren av en bestemt adresse. Slik lagring representerer et meget begrenset inngrep i personvernet

[1] www.uninett.no
[2] www.tradlosetrondheim.no
[3] http://www.digi.no/891200/dld-rot-i-drammen#.UIf15NurPbw.email

samtidig som dataene erfaringsmessig fremstår som svært viktige verktøy for politiet. Lagring av denne type data kan på mange måter sidestilles med registreringsplikten for sim-kort, jfr ekomforskriften § 6-2. For sim-kort har myndighetene bestemt at man i Norge ikke skal ha fri mulighet for anonym kommunikasjon ved at det er innført en registreringsplikt for alle abonnenter.

At inngrepet er beskjedent underbygges også av tilsynets forslag om at politiet fortsatt skal kunne innhente denne typen data uten rettens beslutning da dataene ikke er taushetsbelagt for politiet, jfr ekomloven § 2-9, 3. ledd.

Hvilke sikkerhetskrav som skal stilles til de lagringspliktige er pr dags dato ikke avklart. Det foregår en parallell prosess vedrørende dette. Men man kan med utgangspunkt i vårt syn på den lave graden av sensitivitet til data knyttet til internettaksess, stille spørsmål om hvorvidt denne typen data bør underlegges samme sikkerhetskrav som de øvrige datatypene som skal lagres etter direktivet. Sikkerhetskravene kan ha en direkte innvirkning på vurderingen av hvorvidt kretsen av lagringspliktige skal utvides. Etter Kripos' syn er det forsvarlig å underlegge lagring av internettaksess i et enklere sikkerhetsregime enn de øvrige data. Det samme vil gjelde krav til overlevering til politiet og responstid for denne gruppen subjekter.

Tilsynet har i pkt 3.3.2 hevdet at tilbydere av private nett kan lagre frivillig selv om de ikke pålegges lagringsplikt. Etter Kripos' syn er dette et vel optimistisk og enkelt utgangspunkt. For det første må man anta at den generelle personvernsdebatten som har vært rundt direktivet de siste par år medfører at fokuset på sletting av data vil resultere i at bedrifter/institusjoner som tidligere lagret data frivillig, nå vil ha en mer restriktiv holdning til lagring av data de ikke er pålagt å lagre. For det andre vil lagring av denne typen data trolig kreve konsesjon etter personopplysningsloven. Det vises også til den forventede endring av EU's personvernsdirektiv som vil kunne ha betydning i denne sammenheng[4].

Lagringsplikten for internettaksess kan utvides enten gjennom forskriften eller gjennom enkeltvedtak. Etter Kripos' syn er det lite hensiktsmessig å benytte enkeltvedtak når man allerede nå ser at store grupper subjekter bør omfattes av lagringsplikten.

Dette innebærer at offentlige institusjoner som eksempelvis universiteter, kommuner, bibliotek mv må underlegges lagringsplikt i den grad de tilbyr internettaksess som er allment tilgjengelig. Det samme må gjelde for private bedrifter som hoteller, flyplasser, NSB mv. Det vises til at man i Danmark har innført en langt videre definisjon av tilbyderbegrepet, hvor også andre enn teletilbydere er pålagt lagringsplikt. Slik Kripos oppfatter dette er også alle tilbydere av internett aksess ("hotspots") underlagt lagring[5].

Basert på dette er Kripos klare vurdering at enhver bedrift/institusjon som tilbyr internettaksess eksternt må underlegges lagringsplikt for denne typen data for at formålet med lagring skal oppnås. I praksis vil ikke dette nødvendigvis kreve mer enn at aktørene må innføre autentiseringsløsninger slik at brukerne kan identifiseres, og at disse dataene lagres i 6 måneder. Autentiseringsløsninger er allerede i bruk i mange av disse nettene.

---

[4] http://www.idg.no/computerworld/article238287.ece

[5] http://www.itst.dk/tele-og-internetregulering/forbrug-og-telefoni/krav-til-udbydere/generel-vejledning-om-udbyderbegrebet

3. Tilbyder av tjenester på applikasjonsnivå
For kategori 3 er situasjonen at flere og flere tjenester blir applikasjonsbaserte. Man er avhengige av en forskrift og et regime som tar høyde for disse utviklingstrekkene.

Det erkjennes at det innen denne kategorien kan være en utfordring å trekke klare grenser for hvem som skal lagre. Markedene og teknologiene er i stadig endring. For Kripos er det imidlertid viktig at man allerede nå, ved vedtagelse av forskriften, trekker opp noen klare rammer og gir klare signaler. Skal lagringens formål oppnås må man også være villige til å regulere deler av dette tjenestemarkedet.

For å kunne mene noe nærmere om grensedragningene her har Kripos valgt å dele denne kategorien opp i noen undergrupper, nærmere bestemt slik;

a) Tilbydere av kommunikasjonstjenester med kontor i Norge (eks Opera, Microsoft, Yahoo).
b) Tilbydere av kommunikasjonstjenester som innretter sin virksomhet direkte mot det norske telemarkedet (eks Gmail).
c) Tilbydere av tjenester uten noen tilknytning til Norge (eks en russisk epostleverandør).

Gruppe a – tilbydere med base/tilstedeværelse i Norge
Kripos mener at tilbydere som har kontor/tilstedeværelse i Norge må underlegges lagringsplikt for de datatyper direktivet krever. Eksempler på dette er epostleverandørene Microsoft og Yahoo som etter Kripos' syn må pålegges lagringsplikt for epost-data.

Som fremholdt av enkelte tilbydere på forskriftsmøtet i august fremstår det som lite konsekvent å pålegge norske tilbydere lagringsplikt samtidig som andre store norsk-etablerte tilbydere av tilsvarende tjenester på det norske marked er unntatt. En slik deling fremmer heller ikke lagringens formål, nemlig å gi politiet mulighet for tilgang til data som faktisk finnes og skriver seg fra kommunikasjon i norsk nett/marked.

Et annet eksempel er Opera software som tilbyr en nettleser for smarttelefoner (applikasjonstjeneste). Slik denne tjenesten fungerer, vil man uten lagring ikke kunne identifisere den reelle brukeren når Opera programvare benyttes[6]. Litt forenklet kan man si at man gjennom etterforskning kan finne ut at en IP-adresse som er benyttet stammer fra Opera, men man klarer ikke å finne ut hvem som har foretatt den aktuelle trafikken. Uten pålagt lagring for internettaksess fungerer dette som en anonymiseringstjeneste. Selskapet er et norsk selskap, men utfordringen er internasjonal siden hvem som helst kan bruke denne programvaren. Kripos mottar regelmessig henvendelser om dette fra utenlandske politimyndigheter.

Gruppe b - tilbydere som innretter sin virksomhet direkte mot norsk telemarkedet
Etter Kripos' syn er dette en gruppe som er vanskelig å avgrense/definere. Gruppen kjennetegnes ved at kommunikasjonstjenestene tilbys tydelig mot det norske

[6] Se også kommentarer til pkt 4.3.7 vedr Opera software

telemarkedet, eksempelvis med markedsføring, nettsider som retter seg mot norske brukere osv.

På den ene siden kan det fremstå som problematisk å pålegge selskaper som ikke er representert i Norge en lagringsplikt etter norsk lov fordi slike pålegg vil bli vanskelig å håndheve. Samtidig er det klart at en lagring vil være sterkt ønskelig ut fra en formålsbetraktning.

I mobilmarkedet har Kripos hatt utfordringer med selskaper som Lycamobile som ikke har et norsk kontor, men som tilbyr tjenester i Norge. Denne typen virksomhet er det enda lettere å tilrettelegge for på internettbaserte tjenester hvor man ikke på samme måte er avhengig av en norsk infrastruktur (eks mobilnett). Dersom man ikke underlegger denne typen selskap lagringsplikt, vil man kunne få tilstander hvor i realiteten norske tjenester etableres i utlandet for å unngå lagringsplikt.

Siden denne gruppen er både vanskelig å avgrense, og fordi håndhevingen kan fremstå som problematisk, mener Kripos at det mest nærliggende vil være å avvente regulering inntil man ser hvilken vei utviklingen går. Post- og teletilsynets vedtaksmulighet vil være et alternativ i tilfeller som viser seg særlig nødvendige å regulere.

Gruppe c - tilbydere uten noen tilknytning til Norge
Kripos mener at det innenfor det norske regelverket er vanskelig å pålegge lagringsplikt for selskaper som ikke har noen tilknytning til Norge. Man må ut fra en harmonisering av regelverk internasjonalt legge til grunn at de pålegges lagring i landet hvor de operer fra, og at man i disse tilfellene da må innhente de relevante data gjennom rettsanmodninger til landets myndigheter.

Kommentarer – utkastets kap 3
Temaet "hvem skal lagre" er i hovedsak berørt i kapitel 3 i tilsynets utkast. Der foreslår man ingen utvidelse (eller innskrenkning) av den krets lagringspliktige som følger av utgangspunktet i ekoml § 2-7a *"....tilbyder av elektronisk kommunikasjonsnett som anvendes til offentlig elektronisk kommunikasjonstjeneste og tilbyder av slik tjeneste....."*. I realiteten innebærer dette at hoveddelen av de behov Kripos har påpekt over ikke er tatt til følge. Vi fastholder våre anførsler over og har i tillegg noen særlige kommentarer til det som anføres av tilsynet:

- Tilsynet er gitt en klar hjemmel til å pålegge andre lagringsplikt i ekoml § 2-7a, 2. ledd, der slik utvidelse er nødvendig *"..for å oppnå formålet med bestemmelsen"*. I utkastets 3.3.1. argumenteres det likevel med at det må foreligge særlige grunner før kretsen endres og det vises blant annet til at man ut fra direktivets historie må være varsom med å endre kretsen av lagringspliktige subjekter gjennom forskrift. Kripos mener tilsynet her er for passive og ikke i tilstekkelig grad følger opp lovens ordlyd. Den "*særlige grunn*" tilsynet etterlyser er klart angitt i loven, nemlig oppnåelse av lovens formål. Det kreves ikke grunner ut over dette. Det forhold at implementeringen var gjenstand for diskusjon og i sin form var et resultat av et politisk kompromiss er ikke unikt for denne lovendringen, og kan ikke brukes som argument for passiv bruk av en klar ordlyd.

- Tilsynet legger stor vekt på de pliktsubjekter som følger av ekoml § 2-7a, 1. ledd og de tilhørende definisjoner i lovens § 1-5. Dette er et naturlig utgangspunkt. Imidlertid må man etter Kripos' vurdering – i større grad enn det tilsynet gjør – se hen til at definisjoner og tilhørende forarbeider er skrevet for å ivareta helt andre hensyn enn de som skal ivaretas ved innføring av lagringsplikten i ekoml § 2-7a. Det betyr at de vurderinger og den praksis som er relevant for dagens definisjoner ikke nødvendigvis har noen overføringsverdi når man skal gjøre en fornuftig avgrensning av de lagringspliktige etter ekoml § 2-7a. Det er nettopp derfor man er gitt mulighet til å endre kretsen av lagringspliktige ved forskrift.

- Kripos er tilfreds med tilsynets standpunkt knyttet til innskrenking av kretsen lagringspliktige, jf utkastets punkt 3.3.3. Det er imidlertid nødvendig å kommentere noe av den argumentasjon som benyttes idet den kan tolkes som utrykk for en tolkning av rettstilstanden som ikke har gode grunner for seg. Tilsynet anfører at en konsekvens av innskrenking vil være at man ikke kan benytte straffeprosesslovens §§ 210b og § 210c som hjemmel til på hente ut data. Dette er Kripos enig i. Uthenting etter disse bestemmelser er avgrenset til data som er lagringspliktige og besittes av lagringspliktig tilbyder etter ekoml § 2-7a. En utvidelse eller innskrenking av lagringspliktige subjekter vil således påvirke nedslagsfeltet for uthentingsbestemmelsene i straffeprosessloven § 210b og § 210c.

  Samtidig må det etter Kripos syn være klart at politiets mulighet for innhenting av data - etter de alminnelige regler i straffeprosessloven §§ 203, 205 og 210 - ikke kan være avskåret for ikke-lagringspliktige data eller som besittes av subjekter som ikke omfattes av ekoml § 2-7a. Et motsatt syn vil representere en helt ny rettstilstand som vil bryte med en grunnleggende forutsetning for all kriminalitetsbekjempelse, nemlig muligheten til fri bevisinnhenting. En slik drastisk konsekvens av implementeringen og de nye særbestemmelser for uthenting i straffeprosessloven §§ 210b og 210c kan ikke legges til grunn uten at det er tydelig vurdert og uttalt. En kan ikke se at dette er tilfelle. Det samme må gjelde for de tilfeller der tilsynet fritar en tilbyder med hjemmel i straffeprosessloven § 2-7a, 2. ledd. En følger tilsynets argumentasjon rundt fortsatt taushetsplikt og manglende fritaksmyndighet i slike tilfeller, men mener at rettstilstanden ikke kan forstås slik at det har som resultat at politiet er avskåret fra tilgang til data som tilbyder måtte besitte uavhengig av lagringsplikten. Det må være åpenbart at en slik konsekvens ikke har vært lovgivers mening, og dersom forståelsen opprettholdes av tilsynet bør det etter Kripos mening ha som konsekvens at man foreslår nødvendige regelendringer for å avhjelpe dette.

- Tilsynet åpner for å utvide kretsen av lagringspliktige, men mener dette bør skje ved enkeltvedtak da spekteret av virksomheter gjør det lite hensiktsmessig å regulere dette ved forskrift. Kripos mener tilsynet er for passive. Behovet er allerede signalisert. En utvidelse ved forskrift gir muligheter for å trekke rammer og å gi signaler på en helt annen måte enn ved enkeltvedtak. Dette er viktig både i forhold de som besitter data og forhold til de som skal ha tilgang til data. Se også våre kommentarer til lagringspliktige subjekter for internettaksess ovenfor.

4. HVA SKAL LAGRES

Hvilke data som skal lagres fremkommer av direktivets art 5 sammenholdt med beskrivelsen i Prop. 49 L, pkt 8.5. I tilsynets utkast er temaet hovedsakelig berørt i kapitel 4. Til det som fremgår der har vi følgende særlige merknader:

Kommentarer – utkastets pkt 4.1 og 4.2
Kripos mener at for at formålet med lagringen skal oppfylles, kan det ikke velges en fragmentarisk lagring av data som resulterer i at politiet må henvende seg til en rekke lagringspliktige for å få et komplett sett med data for èn kommunikasjonsident, eksempelvis trafikkdata for et bestemt telefonnummer eller epostadresse.

For at de lagrede data skal være et effektivt verktøy for politiet, må lagringsløsninger og overleveringsprosedyrene til politiet være enkle når det først foreligger et formelt grunnlag som gir tilgang de aktuelle dataene. Dette aktualiserer seg særlig når antallet lagringspliktige øker. I dagens løsning for telefoni har data vært lagret av netteier, og politiet har derfor kun hatt et mindre antall tilbydere å forholde seg til for å innhente trafikkdata. Netteier har lagret både data som er generert i eget nett (trafikkdata og lokasjonsdata), samt roamingdata uavhengig av hvem brukeren har et kundeforhold til. Eksempelvis henvender politiet seg til Network Norway for å innhente alle trafikkdata fra kunder fra Lebara. Dette selv om dataene dels er produsert hos utenlandsk tilbyder, eller i Telenors nett i de geografiske områder hvor Network Norway ikke har eget nett. Lebara besitter i disse tilfellene kun abonnementsdata om egne kunder.

Kripos mener at dagens lagringsmodell er å foretrekke, og er overrasket over at dette alternativet (nytt alt 4) ikke er skissert i tilsynets høringsbrev. Etter Kripos syn kan ansvarsforholdet mellom kundens tilbyder og netteier avklares gjennom en standardisert databehandlingsavtale[7]. Den åpenbare fordelen med dette er et redusert behov for dobbeltlagring, samt at det for politiet vil være færre kontaktpunkter å forholde seg til.

Særlig om abonnementsdata
Høringsbrevet skisserer problemstillingen vedrørende beriking av de lagrede trafikkdata med abonnementsopplysninger hvor den lagringspliktige ikke har disse dataene selv fordi samtaleparten tilhører en annen tilbyder. Dette er en meget relevant problemstilling for politiet, og etter vårt syn undervurderer tilsynet det medarbeid det er for politiet å innhente abonnementsopplysninger fra en rekke tilbydere[8]. Politiet bruker store ressurser på å innhente opplysninger fra de ulike teleoperatører hvor abonnenten har reservert seg mot oppføring i offentlige registre. I våre saker forekommer dette meget hyppig nettopp fordi personer i kriminelle miljøer ikke ønsker at deres telefonnummer skal stå i telefonkatalogen.

For trafikkdata for ett enkelt nummer vil politiet i verste fall måtte henvende seg til samtlige teletilbydere for å innehente abonnementsdata. Politiets anmodninger sendes pr epost og behandles manuelt av teleoperatørene. En rekke av operatørene har ikke krypteringsløsninger tilgjengelige. Prosessen gjentar seg hver gang det innhentes nye trafikkdata, noe som normalt foregår flere ganger i løpet av en etterforskning. Dette

---

[7] Se også Inst 275 (2010-2011), s 4, 2 spalte om "Lagringssted og informasjonssikkerhet" hvor databehandleravtale er omtalt
[8] Høringsbrevet s 9, 3.avsnitt

medfører at det tilsynet omtaler som "antall behandlinger" pr i dag er meget høyt for abonnementsdata. Både politiet og tilbyderne bruker mye ressurser på abonnementsdata, og det paradoksale er at informasjonen ikke er taushetsbelagt for politiet[9]. Det er altså ikke et spørsmål om politiet skal få informasjonen, men hvordan informasjonen skal utveksles.

Dersom ikke tilbyderne selv skal berike opplysninger med abonnementsdata fra andre tilbydere før de overleveres til politiet, må det etter Kripos' syn alternativt etableres en felles løsning hvor politiet kan innhente abonnementsdata. Dette kan tenkes gjort gjennom et bransjeorgan som NRDB hvor politiet kan gjøre databaseoppslag og selv berike de innhentede trafikkdata. En slik løsning finnes eksempelvis i Tyskland[10]. En slik løsning har flere ressursmessige fordeler både for politiet og tilbyderne, og dersom alle forespørsler om abonnementsopplysninger rettes til denne løsningen vil også kravene til statistikkføring av slike henvendelser som etterspørres av EU-kommisjonen[11] kunne møtes.

Kommentarer – utkastets pkt 4.3.6.
Epost-tjeneste leveres i hovedsak i to forskjellige former:

1. Som en ekstra-tjeneste levert av tilbydere av aksess. Et eksempel på dette er at man leier internettaksess hos tilbyderen Telenor, og får, som en del av sitt abonnement, en epost-konto på domenet online.no
2. Som en selvstendig tjeneste, levert av en tilbyder som ikke nødvendigvis tilbyr andre kommunikasjonstjenester. Eksempler på dette er:
    a. Microsoft, som leverer epost-tjenester på blant annet domenene live.no og hotmail.com
    b. Google, som leverer epost-tjenester på domenet gmail.com, men også på egen-registrerte domenenavn som mitt-navn.com

I høringsnotatet legger tilsynet opp til en definisjon av e-post lik "*elektronisk meldingstjeneste som blir tilbudt av en lagringspliktig*". Denne definisjonen tar utgangspunkt i en lagringsplikt, og det forutsettes at man da referer til typetilfelle 1 nevnt over.

Kripos er enig i at det ikke er naturlig å pålegge lagringsplikt for bæreren av epostdata, dvs at eksempelvis Get skal lagre epostdata tilknyttet en kundes bruk av Gmail. Dette kan bare gjennomføres ved en kontinuerlig monitorering av datastrømmen[12], som synes å komme i konflikt med direktivets art 1, pkt 2.

Derimot er det etter Kripos' syn merkelig å knytte lagringsplikten til hvorvidt eposttilbyderen er tilbyder etter ekomloven, jfr vårt typetilfelle 1. Også subjekter som

---

[9] Ekomloven §2-9, 3.ledd
[10] I Tyskland er det opprettet en felles abonnementsdatabase (i regi av Bundesnetzagentur – tilsv etter det opplyste PT i Tyskland) for politiet. Det vil si at politimyndighetene får anledning til å sjekke hvem som er registrert abonnent uavhengig av om vedkommende har reservert seg for oppføringen i telefonkatalog mv. Dette har vist seg meget nyttig siden de har flere tusen ulike teleselskaper å forholde seg til. Via Bundesnetzagentur får politiet kun opplyst navn, adresse og teleoperatør. For ytterligere data (tidspunkt for opprettelse av abonnement, betalingsform mv) må de kontakte teleoperatøren.
[11] DLD art 10 krever at landene skal levere årlige statistikker om bruk av DLD-data. Norge blir spurt om å levere statistikk på bruk av trafikkdata, herunder politiets forespørsler om abonnementsdata. Dette er også inntatt i utkastet til Position paper 16 i EU's ekspertgruppe, se også proposisjonens pkt 15.5.1.
[12] Se også pkt 4.3.7 om NAT

tilbyr eposttjenester uten å være "tilbyder" må pålegges lagringsplikt, jfr våre typetilfelle 2. Både subjekter som har kontor i Norge og subjekter som tilbyr sine tjenester mot det norske markedet må omfattes av forskriften[13].

Definisjonen bør være teknologinøytral, og uavhengig av hvilken protokoll som brukes. Etter Kripos' syn er det mer naturlig å definere lagringsplikten for eposttjenster som "*elektronisk meldingstjeneste som tilbys norske sluttbrukere*". Det vises også til den danske definisjonen av tilbyderbegrepet (*....tilbydere av elektroniske kommunikasjonsnett eller –tjenester til sluttbrukere...*)[14].

Kommentarer – utkastets pkt 4.3.7 - NAT

Bruk av NAT, eller andre tjenester hvor ip-adresser deles på flere brukere, er en utfordring fra et etterforskningsmessig synspunkt. Det medfører at en rekke brukere vil benytte samme offentlige ip-adresse grunnet mangel på ip-adresser (IPv4). Særlig gjelder dette ved mobil internettaksess. Teknisk sett er brukeren koblet til et elektronisk kommunikasjonsnett, og via denne aksessen kobler seg til mellomtjenere som videreformidler kontakt til det nettstedet brukere ønsker å besøke. Dersom man ikke lagrer knytningen mellom den reelle bruker og den offentlige ip-adresse, vil verdien av lagring av internettaksess være minimal når NAT brukes. Problemet vil vedvare inntil IPv6 er fullstending implementert.

Problemstillingen er som oftest at politiet besitter en ip-adresse, og man ønsker å vite hvem som benyttet denne på et gitt tidspunkt. Dersom den aktuelle ip-adressen stammer fra en tilbyder som benytter NAT, må tilbyderen etter det opplyste gjennomgå all ip-trafikk foretatt i sitt system på det aktuelle tidspunktet for å kunne identifisere den aktuelle brukeren. Tilsynet fremholder at registrering av hvilke domener en bruker har vært i kontakt med er det samme som lagring av innhold. Kripos deler ikke denne oppfatningen, og mener det har flere likhetstrekk med lagring av trafikkdata.

Dersom det legges opp til en løsning med ende-til-ende kryptering, vil heller ikke tilbydere se noe av ip-trafikken da denne vil være kryptert. I de tilfeller hvor en konkret ip-adresse skal identifiseres kan tilbydere gjøre et uttrekk av NAT-data for den aktuelle perioden (ofte kun trafikk for noen minutter) kunne identifisere brukeren gjennom knytning til konkrete domenenavn og tidspunkter. Dette har mange likhetstrekk med basestasjonssøk hvor man leter etter en bestemt bruker, men hvor man innhenter trafikk for alle i området for å kunne finne den/de aktuelle samtalene.

Etter Kripos' syn er det derfor forsvarlig at det legges opp til lagringsplikt for NAT-data med det regime som nevnt over, i en overgangsperiode frem til IPv6 implementeres.

Det henvises også til posisjon paper 10 i ekspertgruppen. Position paper 10 er ikke vedtatt, og dokumentet det henvises til er et utkast. Dette dokumentet drøfter ikke NAT-data, men hevder at innsyn i web-strømmer er innholdsdata. Dette er basert på en løsning for identifisering av web-mail, og ville innebære en kontinuerlig monitorering av all web-trafikk hos ISP. Dette er noe helt annet enn løsningen skissert over hvor det kun

---

[13] Se også merknader til pkt 3 – "I hvem skal lagre", underpkt 3 - "Tilbyder av tjenester på applikasjonsnivå"

[14] Bekendtgørelse om udbydere af elektroniske kommunikationsnets og elektroniske kommunikationstjenesters registrering og opbevaring af oplysninger om teletrafik (logningsbekendtgørelsen), §1 (https://www.retsinformation.dk/forms/R0710.aspx?id=2445)

skal hentes ut web-data for perioder hvor det er nødvendig for å identifisere en bruker. Situasjonene er altså ikke sammenlignbare.

Et meget aktuelt eksempel fra Norge er den mobile nettleseren til Opera Software. Ved bruk av denne nettleseren, vil det for brukeren fremstå som man er i direkte kontakt med de nettsteder en ønsker å besøke. Imidlertid er det Opera sine mellomtjenere som er i direkte kontakt med nettstedene, og informasjon og forespørsler blir videreformidlet gjennom disse. Denne type tjenester har som formål å begrense datamengde over mobile nettverk, og er daglig i bruk på mobiltelefoner over hele verden.

Fra etterforskningsmessig synspunkt, vil dette medføre at sporene man jobber ut fra peker mot mellomtjenere og ikke brukeren. Det er derfor nødvendig for tilbyderen som driver mellomtjeneren å være i stand til å knytte sammen nett-aktiviteten med IP-adressen som brukeren er tildelt i sitt kommunikasjonsnett. I dette tilfellet vil Opera ved en gjennomgang av web-trafikk for den aktuelle perioden ikke kunne identifisere hvem brukeren var, men hva som var den opprinnelige ip-adressen. Det er operatøren som eier den opprinnelige ip-adressen som har kundeopplysningene som vil kunne identifisere den reelle brukeren.

Kommentarer – utkastets pkt 4.3.9 – lokaliseringsdata ved start/slutt

Tilsynet foreslår at lokaliseringsinformasjon ved kommunikasjonens slutt ikke skal lagres, noe som samsvarer med direktivet, men ikke med Prop 49L[15]. Kripos viser til at en rekke andre land, herunder Sverige og Danmark, har også registreringsplikt for lokaliseringsinformasjon ved kommunikasjonens slutt. Behovet for denne typen informasjon er grundig drøftet i den svenske utredningen[16] hvor det fremkommer (s 34);

> *"Liksom utredningen kan regeringen också konstatera att lokaliseringsinformation för kommunikationens början många gånger inte alls är tillräckligt för de brottsbekämpande syftena. Om lokaliseringsinformation för kommunikationens slut inte lagras skulle det vara enkelt att i en kriminell verksamhet vilseleda myndigheterna med negativa följder för utredningsarbetet. Detta har också beaktats i exempelvis den danska regleringen, som föreskriver lagringsskyldighet för lokaliseringsuppgifter även rörande kommunikationens slut. Information om var en kommunikation avslutades kan vara lika värdefull som information om var den påbörjades. Mot bakgrund av ovanstående får det enligt regeringens mening anses stå klart att det finnas ett påtagligt behov av att lagra lokaliseringsuppgifter även vid kommunikationens slut."*

De samme forhold som gjøres gjeldende i Sverige er like aktuelle i Norge, og Kripos slutter seg til drøftelsen i den svenske proposisjonen og mener at lokaliseringsinformasjon ved kommunikasjonens slutt må lagres.

Tilsynet hevder også at lagring av lokaliseringsinformasjon ved kommunikasjonens slutt vil medførte økte kostnader, uten at disse kostnadene spesifiseres. Det er derfor vanskelig å vurdere hvilken konsekvens dette har.

---

[15] I utkastet til forskriftstekst §2-3, pkt 10 er likevel lokaliseringsinfonnasjon for kommunikasjonens slutt inntatt
[16] Svensk Prop 2010/10:46, s 33-34

5. TILRETTELEGGING / UTHENTING

Hvordan de lagringspliktige skal tilrettelegge for utlevering til politiet og hvordan denne utleveringen skal skje, er forhold av stor betydning for politiet. Formålet med lagringen vil ikke oppnås dersom lagringsplikten ikke samtidig følges av et regime som sikrer at det legges til rette for og kan gjennomføres en **sikker**, **rask** og **praktisk god** overlevering av **korrekte** data. Dette stiller særlige krav til de lagringspliktige, men også krav til politiet i forhold til et tilrettelagt system henvendelser og mottak.

Det er tidligere i prosessen presenteret noen utgangspunkter fra Kripos' side vedrørende disse sider av implementeringen. Hoveddelen av disse står fremdeles ved lag og gjentas her som del av vårt høringssvar:

1. Kvalitet
Prosessen hos lagringspliktig (lagring/tilrettelegging/utlevering) må være underlagt et slikt regime at politiet kan legge til grunn at overleverte data er korrekte. Om nødvendig må lagringspliktig kunne vise dette.

2. Kontaktpunkter hos lagringspliktige
Alle lagringspliktige må ha kjente og tilgjengelige kontaktpunkter for utlevering, enten hver for seg eller i fellesskap med andre lagringspliktige.

3. Tilgjengelighet hos lagringspliktige
Alle kontaktpunkter for lagringspliktige må være tilgjengelige for utlevering;

i normaltilfellene	innenfor ordinær kontortid (mandag til fredag fra kl 0800 til kl 1600)
i akuttilfellene	døgnkontinuerlig

Med "normaltilfellene" menes de situasjoner hvor man følger hovedregelen for utlevering av data i den forstand at utlevering begjæres for og behandles av retten innenfor ordinær kontortid.

Med "akuttilfellene" menes de situasjoner hvor man ikke kan avvente behandling innenfor rettens ordinære kontortid og derfor benytter seg av politiets hastekompetanse (stprl § 210b, 5. ledd, jf § 210, 2. ledd) eller eventuelt Oslo tingretts døgnåpne service (stprl § 210b, 4. ledd). Det må også gjelde tilsvarende der utlevering kreves med "nødrett" som begrunnelse.

4. Replikeringstid
Alle lagringspliktige må ha et system for replikering (oppdatering) av lagrede data som sikrer;

i normaltilfellene	replikering en gang i døgnet
i akuttilfellene	replikering "der og da" av den type data som etterspørres

5. Responstid
Tidsfrister regnet fra lagringspliktig mottar anmodning om utlevering til svar mottas hos politiet;

i normaltilfellene	i løpet av en virkedag (ved henvendelser fredag vil det si svar i løpet av ordinær kontortid mandag)
i akuttilfellene	snarest mulig

6. Kontaktpunkter hos politiet
I normaltilfellene skal utlevering skje til aktuelt kontaktpunkt for politiet (27 distrikter + PST, ØKOKRIM og Kripos med egne kontaktpunkter og leveringsadresser). Bestiller skal opplyse om rett kontaktpunkt/leveringsadresse (og skal også sende kopi av anmodning til kontaktpunkt).

I akuttilfellene avtaler lagringspliktig utleveringsadresse med bestiller.

Det er naturlig at kontaktpunktene gjøres ansvarlige for den registrering av bruk som er forutsatt ved implementeringen. Det vises blant annet til proposisjonens pkt 15.5.1 om statistikkføring.

7. En felles struktur
All utlevering av data skal skje etter en omforenet struktur som er felles for samtlige lagringspliktige. Det vises til tidligere oversendt forslag fra Kripos til hvordan dette kan løses pr datatype.

8. Overføringsmåte
Data overføres fra lagringspliktig til politiet gjennom kryptert elektronisk oversendelse. Krypteringsløsningen må være ensartet for alle lagringspliktige (samme type kryptering).

9. Tilrettelegging før introduksjon
Introduksjon av nye tjenester som genererer lagringspliktige data kan ikke iverksettes før det er tilrettelagt for utlevering.

10. Brukerforum.
For å sikre en mest mulig smidig implementering - og at regelverk og teknologiske løsninger fortløpende justeres i forhold til erfaringer og utvikling - er det viktig med løpende dialog mellom de involverte. Det foreslås derfor etablering av et "brukerforum" bestående av representanter for de bransjer /myndigheter som berøres, typisk representanter fra lagringspliktige, tilsynet, politiet og eventuelt påtalemyndigheten. Forumet bør forankres og gis et mandat og bør settes i funksjon i tilknytningen til implementeringen og forberedelsen av denne.

Kommentarer – utkastets kap 6

I tilsynets utkast er forhold knyttet til tilrettelegging og uthenting hovedsakelig berørt i kapitel 6. En gjennomgang av anførslene der sammenholdt med punktene over nødvendiggjør noen særlige kommentarer:

- Kripos ser på det som viktig at de mest sentrale forhold knyttet til tilrettelegging og utlevering er klart fastsatt i forskrift. Tilsynets forskriftsutkast berører flere av de forhold Kripos oppfatter som viktige. Noen er imidlertid utelatt, herunder ovennevnte punkt 9. Etter vår vurdering er det viktig at det sammen med introduksjon av nye tjenester følger en plikt til samtidig tilrettelegging for uthenting av lagringspliktige data.

- I utkastets punkt 6.4.4 behandler tilsynet krav til tilgjengelighet og responstid. Kripos har uttalt seg om sine vurderinger av behovet her i ovennevnte punkter 3 og 5. Det synes klart at tilsynet og Kripos her vekter de forskjellige hensyn ulikt.

  For Kripos er det avgjørende at det etableres en ordning som sikrer politiet tilgang til data når behovet faktisk oppstår. I akuttilfelle betyr det tilgang umiddelbart. At en slik ordning koster penger og (forhåpentligvis) sjelden vil bli benyttet endrer ikke behovet. Behovet vil antakelig melde seg i de aller mest alvorlige sakene og konsekvensene av manglende tilgang kan da bli tilsvarende alvorlige. Kostnadene ved en slik ordning vil avhenge av hvordan den organiseres. En har forståelse for at en døgnbemanning for hver enkelt tilbyder ikke er en gjennomførbar ordning, men mener tilsynet i større gard bør pålegge tilbydere ordninger som sikrer politiets behov i akuttilfeller. I dette ligger krav til sikkerhet, krav til felles løsninger osv. En responstid på to til tre dager – som foreslått – synes vanskelig forenelig med de behov som kan oppstå og samfunnets forventninger til politiets kriminalitetsbekjempelse.

- I den samme diskusjon om responstid i akuttilfelle blander tilsynet inn regler hentet fra straffeprosesslovens kap 16a om kommunikasjonskontroll. Kripos oppfatter tilsynets argumentasjon dit hen at disse regler avhjelper politiets behov for kort responstid i akuttilfelle da disse er alternative og gir politiet de tilnærmet samme muligheter til datainnhenting. Det tilsynet skriver om dette synes basert på en uriktig forståelse av straffeprosessloven.

  Reglene i kap 16a er et særlig regelsett om skjult metodebruk. Kapitelet stiller opp særlige vilkår for bruk, og saksbehandlingen er også særegen. Tilsynet skriver blant annet at straffeprosessloven § 216b, 2. ledd, bokstav d[17] vil avhjelpe politiets behov i akuttilfelle, med noen få unntak knyttet til strafferamme og angitte særbestemmelser. Det vises i den forbindelse til at man ved bruk av regelsettet kan pålegge lagringspliktige en bistandsplikt.

  Generelt til dette kan bemerkes at muligheten til å pålegge en plikt til bistand er svært lite verdt så lenge man ikke har noen å kontakte – og så lenge det ikke er oppstilt regler for hva plikten krever av tilgjengelighet og responstid ligger det i realiteten ikke mer i denne plikten enn i plikten til å tilrettelegge for lovbestemt

[17] Tilsynet viser til bokstav b men dette må åpenbart være en feilskrift for bokstav d.

tilgang etter ekoml § 2-8. Videre kan det særlig bemerkes at det tilsynet skriver om muligheten til basestasjonssøk hjemlet i bestemmelsen er misforstått. Denne bestemmelse hjemler ikke slike søk, idet det er et generelt krav for bruk av bestemmelsen at mistenktes kommunikasjonsanlegg må være identifisert. Tilsynet unnlater videre å nevne at bestemmelsen kan kun brukes på kommunikasjonsanlegg som besittes eller brukes av mistenkte selv. Dette er en klar begrensning i forhold til de ordinære uthentingsreglene i straffeprosessloven § 210b og 210c som åpner for innhenting av data tilknyttet saker uten en bestemt mistenkt og tilknyttet kommunikasjonsanlegg som er brukt av andre enn mistenkte. Til slutt nevnes at særvilkårene i straffeprosessloven § 216c heller ikke er kommentert av tilsynet, herunder kravet om at oppklaring i vesentlig grad må bli vanskeliggjort uten bruk av den aktuelle metode.

Samlet sett fremstår tilsynets argumentasjon som mangelfull og forslaget derfor dårlig begrunnet. Kripos kan ikke se at henvisningen til strpl kap 16 a har noen relevans i diskusjonen rundt behovet for responstid og tilgjengelighet i akuttilfeller.

- I utkastets punkt 6.4.5 slår tilsynet fast at lagringspliktiges ansvar ikke omfatter forsendelse til politiet. Kripos bemerker at begge uthentingsbestemmelser i straffeprosessloven bruker uttrykket "*pålegge utlevering*". En naturlig forståelse av dette trekker etter vår oppfatning i retning av at ansvaret ikke nødvendigvis avsluttes ved tilgjengeliggjøring hos lagringspliktig.

6. SÆRLIGE KOMMENTARER

Under følger særlige kommentarer til enkeltpunkter i tilsynets utkast som ikke er berørt i kapitlene over. I tillegg følger også særlige kommentarer til selve forskriftsteksten.

Kommentarer – utkastets pkt 3.4

I høringsnotatet fremgår det at Samferdselsdepartementet "...følger opp hvorvidt Svalbard skal unntas fra lagringsplikten.", uten at det fremgår noen begrunnelse for hvorfor dette vurderes. Kripos vil derfor benytte anledning til å fremheve at vi mener lagringsplikten åpenbart må gjelde også på Svalbard. Vi er kjent med at Svalbardlovens § 2 forutsetningsvis innebærer at man særskilt skal vurdere behovet for at bestemmelsene gis anvendelse på Svalbard, men det kan etter vår oppfatning ikke være tvilsomt at det foreligger et behov.

Moderne telekommunikasjon er i liten grad begrenset av geografisk plassering og jurisdiksjonsgrenser og en operatør som etablerer seg på Svalbard vil kunne tilby tjenester både til det norske fastlandet og internasjonalt. Dette taler i seg selv for tilsvarende lagringsplikt på Svalbard som i Norge for øvrig. I tillegg kommer det faktum at det knapt er noen del av verden som ikke er undergitt et eller annet lagringsregime. Dersom Svalbard skulle være unntaket vil dette skape et "rettstomt" rom som vil kunne tiltrekke seg ulovlig aktivitet nettopp fordi sporingsmulighetene er mindre. Denne bekymring forsterkes av at Svalbards spesielle folkerettslige status gjør at

det er mindre kontroll med hvem som etablerer seg der, enn det er både i Norge for øvrig og de fleste andre steder i verden. Det er for eksempel ingen innreisekontroll.

Kripos mener derfor at lagringsplikten må gjelde også på Svalbard.

Kommentarer – utkastets pkt 5.4
Taushetsplikt hos lagringspliktig knyttet til dataenes behandling er et viktig punkt for politiet. Kripos er glad for at tilsynet påpeker behovet for klare regler, men mener tilsynet må følge opp dette i større grad enn å legge *"....til grunn at det er, eller vil bli etablert slik taushetsplikt med hjemmel i annen lov"*.

Kommentarer – utkastets kap 7
Implementeringen av DLD blitt utsatt flere ganger, og det kan ikke utelukkes flere utsettelser basert de innspillene som har kommet i møter Kripos har deltatt i. I mellomtiden har Datatilsynet blant annet pålagt Netcom sletting av trafikkdata som er eldre enn 3 måneder (endring fra 5 måneder) basert på dagens regelverk. I påvente av innføringen av DLD lider etterforskningen av straffesaker av manglende datalagring. Etter Kripos syn bør lagringstiden av eksisterende data settes til 6 måneder fra og med 01.07.2012 uavhengig hvor langt de øvrige prosesser har kommet. Det vil uansett ta noe tid etter at lagringstiden økes før tilbyderne besitter 6 måneder gamle data.

Kommentarer – utkastets pkt 8.2.
Det er ikke mulig i dag å tallfeste de økonomiske konsekvenser implementeringen vil ha for politiet. Det endelige krav til lagring og utlevering må på plass før kalkyler av tilstrekkelig kvalitet kan oppstilles. Generelt kan bemerkes at det for politiet vil være kostnader knyttet til investering og drifting av nødvendige systemer, personell- og administrasjonskostnader knyttet til begjæring om og uthenting av data, samt kostnader til bearbeiding, analyse og bruk av data i sak.

Kommentarer til forskriftsteksten:

Kommentarer – forskriftens §2-4 (Internettelefontjeneste) og §2-6 (E-post)
Det må inntas krav om lagring av benyttede ip-adresser for avsender og mottaker av kommunikasjonen for at brukeren skal kunne identifiseres.

Kommentarer – mislykkede og tapte anrop – forskiftens §§ 2-2 (fasttelefontjeneste), 2-3 (mobiltelefontjeneste), 2-4 (internettelefontjeneste)
Kripos er kjent med vurderingene og de foreløpige konklusjonene i EUs ekspertgruppes Position Paper 9[18] vedrørende mislykkede anrop. Det må fremgå av forskriftsteksten at det foreligger lagringsplikt for denne typen data såfremt data om dette er tilgjengelig i den lagringspliktiges nett. Slik teksten nå fremstår kreves det at den lagringspliktige først skal lagre data såfremt data logges, lagres og blir behandlet av den lagringspliktige. Det kan tilsynelatende gi uttrykk for en grad av valgfrihet, noe som trolig ikke er hensikten.

[18] Position Paper No 9 "Closer understanding of the term "unsuccessful call attempt" (versjon 14.03.11), ikke vedtatt

Kommentarer – forskriftens § 4-1

I forskriftens § 4-1 har tilsynet foreslått en bestemmelse som skal inneholde en uttømmende liste av tilfelle hvor lagringspliktige data kan behandles. Kripos kan ikke se at nødrettsgrunnlag omfattes av bestemmelsen og mener det bør gå klart fram av bestemmelsen at behandling også kan skje på slikt grunnlag.

Med hilsen

Ketil Haukaas
assisterende sjef

Saksbehandlere:
Padv Reinert M Ottesen Tlf.: 23208668 / 95295018 reinert.ottesen@politiet.no

Pob Rune U. Reitan Tlf.: 23208665 / 41535804 rune.utne.reitan@politiet.no

Kopi til:
Riksadvokaten
Politidirektoratet

POLITIET

Post- og teletilsynet
Postboks 93
4791 LILLESAND

Sendt elektronisk til firmapost@npt.no

Deres referanse	*Vår referanse*	*Dato*
1102068-22 – 417.1	201200206	25. april 2012

DATALAGRINGSFORSKRIFTEN – TILLEGG TIL HØRINGSSVAR FRA KRIPOS

Det vises til telefonsamtale med Hans Olav Røyr mandag 16. april 2012 hvor det ble avtalt at Kripos skulle ettersende et tillegg til høringsuttalelsen vedrørende datalagringsforskriften.

Kripos har blitt oppmerksom på at det er et viktig forhold som ikke er omtalt i høringsbrevet fra tilsynet. Dette gjelder politiets mulighet for å gjennomføre IMEI-søk hos tilbyderne for mobiltelefontrafikk.

Et IMEI-søk innebærer som kjent at politiet forespør tilbyderne om hvilke anropsnummer som er benyttet sammen med et konkret telefonapparat. IMEI er mobiltelefonens serienummer. Denne typen forespørsler må gjennomføres i de lagrede trafikkdata, og når DLD innføres må søket foretas i dataene som er lagret etter direktivet.

Når politiet beslaglegger en mobiltelefon, vil denne typen undersøkelse gi svar på hvilke andre anropsnummer (simkort) mistenkte kan ha disponert, ved at tilbyderen opplyser om hvilke andre simkort som har vært benyttet sammen med det aktuelle IMEI-nummer. Dette er en meget relevant undersøkelse å foreta. Motsatt er det også mulig å forespørre hvilke telefonapparater (IMEI) som er benyttet sammen med et bestemt anropsnummer. Det gir en oversikt over hvilke apparater mistenkte kan ha benyttet.

Undersøkelsen er også meget aktuell i forbindelse med kommunikasjonskontroll, i tilfeller hvor mistenkte ofte bytter anropsnummer. IMEI-søk er da en av flere muligheter for å finne ut hvilke anropsnummer mistenkte benytter.

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

Politiet gjennomfører anslagsvis 12.000 – 15.000 IMEI-søk pr år[1]. Opplysningene er ikke taushetsbelagt for politiet, jfr ekomloven § 2-9.

Siden politiet ikke vet hvilken tilbyder(e) mistenkte har benyttet, må IMEI-forespørselen rettes til alle tilbydere. Ved dagens løsning, hvor det er netteier som lagrer alle trafikkdata, må forespørselen rettes til de 3 netteierne Telenor, Netcom og NetworkNorway.

Dersom man velger høringsnotatets *løsning 1* hvor det er den enkelte tilbyder som skal lagre sine egne og roamingdata, vil det bety at denne typen forespørsler må rettes til alle de 27 tilbyderne. Dette vil medføre store praktiske og økonomiske konsekvenser for politiet. Tilsynet har i sin oppregning i høringssvaret ikke innregnet "antall behandlinger" for abonnementsopplysninger og IMEI-søk, men ved løsning 1 vil "antall behandlinger" for IMEI-søk 10-dobles siden antall tilbydere som forespørselen må rettes til øker fra 3 til 27 tilbydere.

Dersom man velger *løsning 2* hvor politiet skal kunne uthente basestasjonsdata hos netteier, og det presiseres at det samme også gjelder for IMEI-søk, vil situasjonen bli som ved dagens løsning. Likevel vil man som tidligere bemerket ha problemstillinger knyttet til dobbeltlagring av trafikkdata for mobiltelefon.

Kripos mener derfor, som bemerket i vårt høringssvar av 10. april 2012, at dagens løsning hvor trafikkdata for mobiltelefon og roamingdata lagres av netteier er å foretrekke (*vår løsning 4*) også i forhold til IMEI-søk.

Med hilsen

Ketil Haukaas
assisterende sjef

Saksbehandlere:
Padv Reinert M Ottesen Tlf.: 23208668 / 95295018 reinert.ottesen@politiet.no

Pob Rune U. Reitan Tlf.: 23208665 / 41535804 rune.utne.reitan@politiet.no

Kopi til:
Riksadvokaten
Politidirektoratet

[1] Tallene er basert på et overslag mottatt fra Telenor som i 2011 gjennomførte ca 4000-6000 IMEI-søk på vegne av politiet. Tallene er omtrentlige fordi man ikke fører en nøyaktig oversikt pr søk. Man kan legge til grunn at de øvrige netteiere (Netcom og Network Norway) har omtrent samme antall forespørsler da IMEI-søk som regel rettes til alle netteiere.

POLITIET

Datatilsynet
Postboks 8177 Dep.
0034 OSLO

Deres referanse	*Vår referanse*	*Dato*
11/01149-3	2012/	19.4.2012

Tilsvar – konsesjon til å lagre personopplysninger i medhold av ekomloven § 2-7a

Kripos viser til Datatilsynets henvendelse av 29. mars 2012, hvor det bes om at eventuelle tilbakemeldinger til utkast til konsesjon for lagring av DLD-data sendes tilsynet innen 18. april samme år. Kripos er gitt utsatt svarfrist til 25. april.

Implementering av DLD er et krevende arbeid, hvor flere myndigheter og virksomheter er involvert i prosesser rundt utarbeidelse av regelverk og kontroll- og tilsynsmekanismer, samt fordeling av kostnader. Flere av disse prosessene både påvirker og er avhengig av hverandre. Det har fra Kripos og andre involverte aktører blitt etterlyst en mer samlet behandling av de ulike elementene ved implementeringen. Kripos mener det er en forutsetning for god implementering at man i tilstrekkelig grad avklarer prosessenes betydning for hverandre og undergir dem en nødvendig felles behandling, så også for tilsynets utarbeidelse av konsesjon i medhold av ekomloven § 2-7a.

Som Datatilsynet er kjent med, har Kripos deltatt i prosessen som har ledet frem til konsesjonsutkastet. Kripos har underveis i dette arbeidet påpekt sentrale forhold av betydning for politiets arbeid. Vi ønsker likevel å gi noen merknader i forbindelse med høringen.

Konkrete tilbakemeldinger til konsesjonsutkastet
1. Behandlingsansvarlig
Etter Kripos' oppfatning bør første setning under dette punktet endres til: "Den behandlingsansvarlige virksomhet er den som underlegges lagringsplikt etter datalagringsforskriften eller ved enkeltvedtak."

I denne forbindelse vises det til vårt høringssvar av 10. april 2012 til datalagringsforskriften, se særlig punkt 3. Høringssvaret følger vedlagt.

5. Innsyn jf. merknad om den registrertes rett til innsyn
Punkt 5 i konsesjonen fastslår den registrertes rett til innsyn i alle opplysninger som er lagret om vedkommende, jf. personopplysningsloven § 18. Merknadene gir nærmere presiseringer for innsynsrettens omfang i dette tilfellet.

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

Kripos erkjenner at hovedregelen, jf. personopplysningloven § 18, vil være at den registrerte har krav på innsyn i opplysninger som er registrert om seg selv. Datatilsynet viser i sitt forslag til merknader på dette punktet at eksempelvis straffeprosessloven § 208a om utsatt etterretning vil være et tilfelle hvor øvrig regelverk vil begrense innsynsretten.

Etter vår oppfatning bør teksten på dette punkt endres til en mer generell formulering, slik at misforståelser ikke oppstår. Det utvilsomt at innsynsretten vil begrenses av særlovgivningen, som eksempelvis straffeprosessloven, på langt flere områder enn ved utsatt etterretning etter straffeprosessloven § 208a. Opplysninger om hvorvidt politiet har forespurt om data fra en lagringspliktig, reguleres av underretningsreglene i straffeprosessloven. Det må derfor eksplisitt fremkomme at denne typen opplysninger ikke skal gis av lagringspliktig.

6.1.1 Innholdsfortegnelse og uthenting av data
Kripos foreslår at det i tilknytning til dette punket i konsesjonen utarbeides en oversikt over hvilke verdier/opplysninger som skal hashes og som således kan innhentes fra politiet i henhold til formålet med datalagringsregelverket. Hvilke verdier som er søkbare er helt avgjørende for politiets nytteverdi av opplysningene. Kripos bidrar gjerne med utarbeidelse av et forslag til hvilke verdier som bør være søkbare for de ulike datatyper som skal lagres.

7.6 Forsendelse av data over landegrensene
Kripos legger til grunn at det på dette punktet, i henhold til konsesjonens virkeområde, henvises til de forsendelser av data som behandlingsansvarlige eller eventuelt databehandler forestår. Politiets behandling av opplysningene etter at de er utlevert reguleres av annen lovgivning, blant annet politiregisterforskriften og kommunikasjonskontrollsforskriften. For å unngå misforståelser, bør dette presiseres.

8. Utlevering av opplysninger
Av annet avsnitt under konsesjonens punkt 8 fremgår det at opplysningene før utlevering skal dekrypteres, for deretter å krypteres med den relevante myndighets offentlige nøkler. For politiet er det avgjørende at det etableres en ensartet overføringsmetode mellom lagringspliktig og politiet.

Det er etter vår oppfatning av stor betydning at man får etablert et felles lagringsformat, jf. forslaget til datalagringsforskrift § 4-3 om tilretteleggingsplikt. Dette for å ivareta sentrale elementer i prosessen, som tilgjengelighet, ensartethet og kvalitet på opplysningene. For en videre gjennomgang av dette spørsmålet vises det igjen til vårt vedlagte høringssvar til datalagringsforskriften.

Merknad vedr. sikkerhetselementer
Til merknadens punkt sikkerhetselementer, under kategorien "søkeelementer" viser Kripos til sine kommentarer i forrige punkt.

Øvrige merknader
Retting av opplysninger
Kripos registrerer at en nærmere presisering av retting av opplysninger er utelatt fra nåværende forslag. Det legges med dette til grunn at problematikken knyttet til retting av

eksempelvis basestasjonsopplysninger på forespørsel fra den registrere bortfaller, og således at den registrerte kun kan kreve å få rettet de typiske kundeopplysningene som navn og adresse.

Behov for videre avklaringer
Som nevnt innledningsvis bes det om at Datatilsynet ser hen til øvrige prosesser for implementering av datalagringsdirektivet i sitt arbeid med ferdigstillelse av konsesjonen for behandling av personopplysninger etter ekomloven § 2-7a.

Kripos stiller seg til disposisjon og bidrar, som nevnt over, ved behov for avklaring av hvilke kategorier av verdier/opplysninger som skal hashes.

Med hilsen

Ketil Haukaas
ass. sjef

Christine Ask Ottesen
seniorrådgiver

Vedlegg: Kopi av Kripos høringssvar til datalagringsforskriften