Innholdsfortegnelse

1. INNLEDNING OG SAMMENDRAG

1.1 Innledning

EU vedtok 15. mars 2006 direktiv 2006/24/EF om lagring av data fremkommet ved bruk av elektronisk kommunikasjon med endring av direktiv 2002/58/EC. Fristen for gjennomføring av direktivet for EUs medlemsland var 15. september 2007. Direktivet åpner for en utsatt implementering av data knyttet til Internett, bredbåndstelefoni og e-post til mars 2009.

Direktivet er foreløpig ikke innlemmet i EØS-avtalen. En av grunnene til dette var at man fra norsk side ønsket å avvente dom fra EF-domstolen i sak C-301/06 Irland mot Ministerrådet og EU-parlamentet. Spørsmålet i denne saken var direktivets rettslige grunnlag. Direktivet er vedtatt med hjemmel i artikkel 95 i EF-traktaten. Irlands påstand var at regelverket skulle vært vedtatt som en rammebeslutning med hjemmel i del VI av EU-traktaten (politi- og strafferettssamarbeidet), mer konkret artikkel 30, 31 (1) og 34 (2).

I dommen av 10. februar 2009 slår EF-domstolen fast at artikkel 95 i EF-traktaten er riktig hjemmel for direktivet. Det vises til at direktivet utelukkende regulerer tilbydernes plikt til å lagre data og ikke inneholder bestemmelser om rettshåndhevendes myndigheters tilgang til eller bruk av opplysningene. Domstolen viser også til at en rekke medlemsstatene etter terroristangrepene 11. september 2001 i New York, 11. mars 2004 i Madrid og 7. juli 2005 i London hadde vedtatt regler om datalagring, og at flere stater hadde planer om å innføre slike regler. Det var betydelige forskjeller mellom statenes lovgivning. I og med at innføring av slike regler ville ha betydelige økonomiske konsekvenser for tilbyderne, ville forskjellene i nasjonal lovgivning ha direkte betydning for det indre marked.

Fra norsk side har man ventet med å ta stilling til innlemming av direktivet til EF-domstolens dom. I dag lagrer tilbyderne i Norge trafikkdata for kommersielle forhold. Trafikkdata er data som er nødvendige for overføring av kommunikasjon i et elektronisk kommunikasjonsnett eller for fakturering av slik overføring. Politiet har mulighet til å få tilgang til disse dataene for å etterforske eller forebygge straffbare handlinger.

Det nye med datalagringsdirektivet er at tilbyderne pålegges en lagringsplikt, at flere data enn i dag skal lagres, at lagringstiden vil bli lengre og at lagring skal foregå for et annet formål – nemlig kriminalitetsbekjempelse. Data som i henhold til direktivet skal lagres er trafikkdata, lokaliseringsdata og abonnements/brukerdata som fremkommer ved bruk av elektronisk kommunikasjon som fasttelefoni, mobiltelefoni og internettaksess, bredbåndstelefoni og e-post. I det etterfølgende benyttes begrepet data som samlebetegnelse for dette. Lagring av data reiser spørsmål knyttet til personvern og kriminalitetsbekjempelse og rammevilkårene for tilbydere av ekomnett og -tjenester. For departementene er det viktig at eventuelle regler om datalagring ledsages av krav til datasikkerhet og personvern. Like regler for tilbydernes plikt til å lagre data er også

viktig for å hindre konkurransevridning, både internt i Norge og i EØS-området. Lovforslagene er derfor utformet i tråd med dette.

1.2 **Kort om innholdet i direktivet**

Formålet med direktivet er å harmonisere lovgivningen om lagring av nærmere definerte data fremkommet ved bruk av elektronisk kommunikasjon. Hensikten er å gi justismyndighetene et verktøy for å avdekke, etterforske og rettsforfølge alvorlig kriminalitet.

Direktivet legger klare føringer for hvem som skal lagre og hva som skal lagres. Direktivet inneholder også bl.a. visse krav til informasjonssikkerhet hos tilbyder. Det er tilbydere av offentlig elektronisk kommunikasjonsnett eller -tjeneste som er pliktsubjekt for lagringen. Hver enkelt tilbyder skal lagre de data som fremgår av direktivet og som produseres når de selv utfører sin tjeneste, det vil si data de har tilgang til. Tilbyderne skal ikke etablere systemer for å kunne lagre data som de ikke har tilgjengelig ved produksjon av tjenesten.

Direktivet overlater til nasjonale myndigheter å ta nærmere stilling til flere viktige spørsmål. Dette gjelder bl.a. spørsmålene om tilgang til og utlevering av, dataene som lagres, lagringstiden (i henhold til direktivet skal den være mellom 6 og 24 måneder), kostnader, hvem som skal føre tilsyn med ordningen og valg av teknologi for lagringen.

I henhold til artikkel 14 i direktivet skal EU-kommisjonen innen 15. september 2010 legge frem for Europaparlamentet og Rådet en evaluering av implementeringen av direktivet og dets innvirkning på økonomiske virksomheter og forbrukere. Kommisjonen skal se på i hvilken grad man så langt har nådd målet med datalagringsdirektivet, for eksempel i hvor stor grad en harmonisering har funnet sted. Den teknologiske utviklingen og statistikk fra medlemslandene skal legges til grunn i vurderingen av om det er nødvendig å endre bestemmelser i direktivet, særlig med tanke på listen over data som skal lagres (artikkel 5) og lagringstid (artikkel 6). Evalueringen skal være offentlig.

1.3 **Tidligere prosess**

Som et ledd i arbeidet med datalagringsdirektivet etablerte Samferdselsdepartementet i 2006 en interdepartemental arbeidsgruppe bestående av Justisdepartementet, Fornyings- og administrasjonsdepartementet, Utenriksdepartementet, Datatilsynet, Post- og teletilsynet og Kripos. Gruppen vurderte direktivet og diskuterte de spørsmålene hvor det i henhold til direktivet er valgmuligheter knyttet til gjennomføringen. Dette gjelder som nevnt blant annet spørsmålene om lagringstid og hvem som skal lagre. Gruppen diskuterte også hvem som bør ha tilgang til data, vilkår for tilgang til data, samt spørsmålet om kostnader. Gruppen utarbeidet ikke noen selvstendig rapport, men arbeidet dannet grunnlaget for dette høringsnotatet. Samferdselsdepartementet har videre vært bistått av en referansegruppe i arbeidet med å komme frem til forslagene om endring i ekomloven. Referansegruppen ble søkt

sammensatt av et representativt utvalg av ekomtilbydere, og bestod av Telenor, NetCom, Tele2, TDC, Telio, Infonett Røros og Lyse Tele. Post- og teletilsynet og Kripos deltok også i referansegruppen.

Med bakgrunn i et ønske om å hindre konkurransevridning, og å finne en så effektiv lagringsløsning som mulig med en så liten økonomisk belastning som mulig for tilbydere av elektroniske kommunikasjonsnett og -tjenester, har Samferdselsdepartementet og Justisdepartementet fått gjennomført to økonomiske utredninger av konsekvensene knyttet til innføring av en lagringsplikt. Den første utredningen ble gjennomført av Teleplan i perioden september – desember 2006. Formålet med analysen var å gjøre en vurdering av kostnader forbundet med en eventuell innføring av en plikt til å lagre data knyttet til lagring av data generert ved bruk av fasttelefoni, mobiltelefoni og internettaksess. Den utredningen skulle gi svar på følgende:

- kostnader for tilbyderne ved ulike modeller for lagring (lagring i en sentral database eller lagring hos tilbyder)
- kostnader for staten ved ulike modeller for lagring
- økonomiske konsekvenser ved innføring av en lagringsplikt på alle kategorier data som EUs datalagringsdirektiv skisserer (avgrenset til lagring av data generert ved bruk av fasttelefoni, mobiltelefoni og internettaksess).
- hvordan og i hvilken grad lagringstiden virker inn på kostnadene
- hvordan og i hvilken grad informasjonssikkerheten virker inn på kostnadene
- muligheten for å kunne benytte infrastruktur og standarder som er etablert/skal etableres hos tilbydere for å kunne utføre kommunikasjonskontroll

Teleplans utredning ble diskutert både i arbeidsgruppen og i referansegruppen. De viktigste funnene i utredningen omtales i notatets kapittel 2.2 og 4.7.

Den andre utredningen ble gjennomført i perioden desember 2007 – februar 2008. Formålet med denne utredningen var å gjøre en vurdering av kostnader knyttet til en eventuell innføring av en lagringsplikt i norsk rett. Det skulle utredes kostnader for alternative lagringstider (6 mnd og 1 år) og utredningen skulle gi svar på følgende:

- tilbydernes investeringskostnader for tilrettelegging av lagringsplikten
- tilbydernes merkostnader knyttet til drift for oppfyllelse av lagringsplikten
- hvordan og i hvilken grad informasjonssikkerheten virker inn på kostnadene
- hvordan lagringstid virker inn på kostnadene

De viktigste funnene i utredningen omtales i notatets kapittel 6 om administrative og økonomiske konsekvenser.

Teleplans utredninger kan lastes ned på Samferdselsdepartementets hjemmeside: www.regjeringen.no/sd

Også andre aktører enn departementene har utredet spørsmål knyttet til eventuell innføring av datalagringsdirektivet i norsk rett. Personvernkommisjonen avga sin rapport *NOU 2009:1 Individ og integritet* i januar 2009 og denne innholder en innstilling

og anbefaling om datalagringsdirektivet, se utredningen punkt 17.6 på side 197-198, jf vedlegg 1 på side 221-223. Innstillingen er å finne på www.regjeringen.no/fad Metodekontrollutvalgets evaluering av lovgivningen om politiets bruk av skjulte tvangsmidler og behandling av informasjon i straffesaker har også et avsnitt om datalagring, jf. NOU 2009:15 punkt20.4. Det vises til nærmere omtale under kapittel 2.4.4. Utredningen finnes på www.regjeringen.no/jd

Direktivets forhold til EØS-avtalen har også blitt vurdert. IKT-Norge overleverte en betenkning til departementene skrevet av professor dr juris Finn Arnesen og professor dr juris Fredrik Sejersted om datalagringsdirektivets EØS-rettslige relevans. De samme professorene utarbeidet, på oppdrag fra Samferdselsdepartementet, i juni 2008 en betenkning om datalagringsdirektivet og EØS-avtalen. Begge disse betenkningene er avgitt før dommen fra EF-domstolen ble avsagt. De er å finne på Samferdselsdepartementets hjemmeside: www.regjeringen.no/sd

EU-kommisjonen nedsatte 25. mars 2008 en ekspertgruppe for blant annet å sikre erfaringsutveksling og diskusjon av sentrale problemstillinger knyttet til implementeringen av direktivet i medlemslandene. Ekspertgruppen har under utarbeidelse flere dokumenter som skal gi veiledning i hvordan medlemslandene skal tolke og tilnærme seg pliktene i direktivet. Dokumentene er såkalte "position papers". De fleste av disse veiledningene er ikke ferdige. Departementene har gjennom EFTA-sekretariatet fulgt arbeidet i ekspertgruppen og har hatt nytte av drøftingene i gruppen i utarbeidelsen av høringsnotatet.

1.4 Høringsnotatets hovedinnhold

I høringsnotatet gjøres det først rede for direktivets innhold, gjeldende rett og praksis for lagring og uthenting av data i Norge i dag. Videre er rettstilstanden og implementeringen av datalagringsdirektivet i andre nordiske land beskrevet, samt litt om situasjonen i andre EU-land. Etter dette drøftes det hvordan datalagringsdirektivet eventuelt kan gjennomføres i norsk rett.

Departementene har vurdert direktivet opp mot Den europeiske menneskerettighetskonvensjonen, og legger til grunn at det er forenlig med kravene som stilles i EMK artikkel 8.

Datalagringsdirektivet fastsetter en plikt til å lagre trafikkdata, lokaliseringsdata og abonnements/brukerdata fremkommet ved bruk av elektronisk kommunikasjon som fasttelefoni, mobiltelefoni, internettaksess, e-post og bredbåndstelefoni. Innholdet, eller informasjon som avslører innholdet i kommunikasjonen, omfattes ikke. En detaljert oppregning av hva som skal lagres fremgår av kapittel 4.4. En eventuell lagringsplikt foreslås nedfelt i ekomloven § 2-8.

Lagringsplikten foreslås eventuelt å gjelde for tilbyder av offentlig elektronisk kommunikasjonsnett eller -tjeneste. Departementene legger til grunn samme definisjon av disse begrepene som i ekomloven. Det vil si at enhver fysisk eller juridisk person

som tilbyr andre tilgang til elektronisk kommunikasjonsnett som anvendes til offentlig elektronisk kommunikasjonstjeneste eller tilbyder av slik tjeneste, skal lagre data. Det legges imidlertid opp til at myndighetene gjennom enkeltvedtak kan pålegge andre enn de som faller inn under tilbyderbegrepet en lagringsplikt dersom dette er nødvendig for å oppnå formålet med bestemmelsen.

Høringsnotatet drøfter i kapittel 4.7 ulike modeller for lagringssted. Lagring hos tilbyder, lagring i en sentral database og mellomløsninger skisseres som mulige alternativer for hvor og hvordan de lagrede data skal oppbevares. De ulike lagringsløsningene har både sine fordeler og sine ulemper. Hovedspørsmålet som må stilles i vurderingen av en sentral databaseløsning, er om det er ønskelig å samle så mye data om bruk av elektronisk kommunikasjon på et sted. Departementene har kommet til at det av personvernmessige årsaker ikke er ønskelig med en sentral lagringsløsning. Departementene er dessuten av den oppfatning at det er tilbyderne som best er egnet til å finne de mest økonomisk effektive, sikreste og hensiktsmessige løsningene for lagring.

Når det gjelder lagringstid skal den i henhold til datalagringsdirektivet være mellom seks måneder og to år. Departementene har valgt å la spørsmålet om lagringstid stå åpent i høringsnotatet. Kapittel 4.8 redegjør både for argumenter som taler for lang lagringstid og argumenter som taler for kort lagringstid.

Direktivet foreskriver at data kun skal utleveres til kompetente myndigheter, og i særlige saker. Departementene foreslår at dette gjennomføres ved en endring i straffeprosessloven § 210 der det fremgår at utlevering bare skal skje til politiet etter avgjørelse av retten. Hensikten med lagringen er å bekjempe alvorlig kriminalitet, og det foreslås derfor at utlevering bare skal kunne pålegges i saker av en viss grovhet (handlinger som kan straffes med fengsel i 3 år eller mer). Visse forbrytelser som har en lavere strafferamme enn tre år kan være særlig vanskelige å etterforske uten å kunne benytte data. Det er således departementenes syn at også andre saker kan vurderes som "særlige saker". Det vises til den foreslåtte uttømmende listen over slike straffebestemmelser i kapittel 4.12.

Departementene foreslår videre at dersom direktivet skal gjennomføres i norsk rett videreføres dagens tilsynsordning med et delt tilsynsansvar mellom Post- og teletilsynet og Datatilsynet. Det må forventes at begge tilsynene får økte administrative kostnader i tilknytning til dette. Når det gjelder øvrige kostnader knyttet til en eventuell gjennomføring av direktivet har det som det fremgår av kapitlene 1.3 og 6 blitt gjennomført flere utredninger om dette. Departementene vil foreta nye vurderinger av kostnadene knyttet til en eventuell gjennomføring av direktivet parallelt med denne høringen. Departementene legger til grunn at dagens kostnadsdelingsmodell, hvor ekomtilbyderne har en tilretteleggingsplikt og dekker kostnadene til denne plikten, mens drifts/uthentingskostnader dekkes av politiet i henhold til avtaler, fortsatt skal gjelde.

2. BESKRIVELSE AV GJELDENDE RETT OG PRAKSIS

2.1 Retten til lagring av data hos tilbyder

Lagring av data fremkommet ved bruk av elektronisk kommunikasjon er som nevnt ikke noe nytt. Allerede i dag behandler, herunder lagrer, tilbyderne trafikkdata for fakturerings- eller kommunikasjonsformål i en periode som er noe kortere enn datalagringsdirektivets minimums lagringstid. Lagring av slike opplysninger medfører behandling av personopplysninger som reguleres av personopplysningsloven. Ekomloven § 2-7 annet ledd oppstiller en *sletteplikt* for trafikkdata når disse ikke lenger er nødvendige til fakturerings- eller kommunikasjonsformål. Politiet har hjemler for tilgang til de opplysningene som faktisk er lagret. En prinsipiell nyskapning med direktivet er at det innføres en plikt til å lagre data og at dette skjer for å imøtekomme myndighetenes behov. En slik lovbestemt lagrings*plikt* vil føre til lik lagringstid hos alle tilbydere for de dataene lagringsplikten gjelder.

Datatilsynet har, med hjemmel i personopplysningsloven § 31 fjerde ledd jf. personopplysningsforskriften § 7-1, gitt tilbyderne konsesjon til å behandle personopplysninger om abonnenters bruk av teletjenester. Formålet med behandlingen er kundeadministrasjon, opplysningstjeneste, fakturering og gjennomføring av tjenester i forbindelse med abonnentens bruk av telenett, inklusive samtrafikkavregning. Generelt gjelder et krav om at den behandlingsansvarlige skal slette eller anonymisere opplysninger som ikke har betydning for formålet. Opplysninger som brukes til fakturering, skal slettes når faktura er gjort opp, eventuelt når klagefristen er utgått. Maksimal lagringstid etter konsesjonens punkt 8 er fem måneder etter at de ble registrert ved kvartalsvis fakturering, og tre måneder etter at de ble registrert ved månedlig fakturering. Dersom en faktura ikke er betalt, eller det er oppstått rettslig tvist om betalingsplikten, kan opplysningene likevel oppbevares inntil kravet er gjort opp eller er rettslig avgjort.

Datatilsynet uttalte våren 2009 at lagring av opplysninger om kundenes internettrafikk, dvs. kobling mellom IP-adresse og abonnement, ikke kan overstige tre uker. Denne type data lagres for å sikre forsvarlig drift, og ikke for fakturering. Datatilsynet har lagt til grunn at tilbyderne har et saklig behov for å oppbevare disse dataene i en kortere periode enn det som gjelder for trafikkdata som benyttes til fakturering. Lagringstiden for denne type trafikkdata er altså vesentlig kortere i dag enn den korteste lagringstid som foreskrives i direktivet.

Det følger av personopplysningsloven § 13 at tilbyder gjennom planlagte og systematiske tiltak skal sørge for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet og tilgjengelighet ved behandling av personopplysninger. Med hjemmel i § 13 fjerde ledd er det i personopplysningsforskriften kapittel 2 gitt utfyllende regler om hvordan informasjonssikkerheten hos tilbyder skal ivaretas. Sikkerhetstiltak må etableres etter en konkret vurdering av de personopplysninger som behandles i forhold til trusler mot informasjonssikkerheten som er til stede. Denne

vurderingen skal foretas av tilbyder med utgangspunkt i et internkontrollsystem for sikkerhet. Det er kravene til dette styringssystemet som beskrives i personopplysningsforskriften kapittel 2, jf. kgl. res. 15. desember 2000 om fastsettelsen av forskriften. Videre gir ekomforskriften §§ 7-1 til 7-3 nærmere regler om hvordan trafikkdata, abonnementsdata og informasjonskapsler (cookies) skal behandles av tilbyderne slik at konfidensialitet sikres.

Ekomloven § 2-8 pålegger tilbyderne en tilretteleggingsplikt for å sikre politiets lovbestemte tilgang til informasjon om sluttbruker og elektronisk kommunikasjon. En lagringsplikt kan imidlertid ikke innfortolkes i tilretteleggingsplikten i § 2-8. Det er presisert i ekomloven § 2-8 tredje ledd at myndigheten kan gi forskrift om lagring av trafikkdata for en viss periode. Denne forskriftshjemmelen er per i dag ikke benyttet.

2.2 Tilbydernes lagringspraksis

Tilbydere logger og lagrer informasjon som er nødvendig for den forretningsmessige driften. Dette er informasjon som er nødvendig for å fakturere sluttbrukere, avregne samtrafikkpartnere, kapasitetsovervåkning og lignende. Trafikkdata genereres i ulike systemer avhengig av hvilke systemer som benyttes for å produsere tjenestene. Dataformatene som benyttes er også ulike avhengig av hvilke systemer som genererer trafikkdata. Det betyr at data ofte konverteres fra det originale formatet (omtalt som CDR-format = Call Detail Record) til andre interne formater tilpasset tilbyderenes systemer for å behandle trafikkdata. Systemene som brukes for å samle inn, lagre, etterbehandle og hente ut trafikkdata, er tilpasset tilbydernes operative prosesser og behov. Det betyr at selv om trafikkdata samles inn og tas vare på, vil de ofte finnes distribuert på flere systemer på ulike formater. Lagringstiden er ulik avhengig av type data og bruksområde.

Verdikjeden for produksjon av ekomtjenester er kompleks. Det er vanlig at tilbydere av telefoni- og internettjenester kjøper tjenester fra andre tjenestetilbydere. I noen tilfeller kjøper disse igjen også tjenesten fra andre tilbydere. Det betyr at data samles inn av en tilbyder og videresendes til en annen tilbyder som igjen fakturerer sin kunde osv. Data kan derfor i perioder være lagret flere steder. Det betyr også at tjenestetilbydere som tilbyr tjenester til sluttbruker, ikke nødvendigvis alene har alle data som lovforslaget krever skal lagres. Eksempelvis har en videreselger som tilbyr mobiltjenester til sluttbruker informasjon om abonnentsdata (navn og adresse), mens nettilbyderen besitter trafikkdata tilhørende samtalebruk. Virtuelle mobiltilbydere (tilbydere uten eget nett – såkalte MVNOer), som i større grad enn rene videreselgere produserer tjenestene sine selv, vil også besitte mesteparten av data vedrørende samtaler. I sistnevnte tilfelle besitter nettilbyderne normalt kun celle-ID og IMEI-nummer, dvs hvilke telefonnummer som kan knyttes til et telefonapparat. IMEI- nummer står for International Mobile Equipment Identifier og hver mobilterminal har et unikt IMEI-nummer.

I mobilnettet kalles en liten gruppe basestasjoners dekningsområde en celle. Celle-ID er identiteten til den cellen i mobilnettverket hvor et mobiltelefonanrop origineres (starter) eller termineres (avsluttes). Når en mobil er i aktiv samtale, vil nettet følge bevegelsene til mobilen fra basestasjonscelle til basestasjonscelle (såkalt hand-over).

Et annet eksempel hvor data lagres flere steder er navn- og adresseinformasjon om den det blir ringt til. I dette høringsnotatet benyttes begrepene A-abonnement om kunden som originerer samtalen, B-abonnement om kunden som mottar samtalen og C-abonnement om en kunde som mottar en viderekoblet samtale. Telefonnumrene til disse betegnes som henholdsvis A-nummer, B-nummer og C-nummer. En tilbyder lagrer kun navn- og adresseinformasjon om sine egne kunder. Dersom A-abonnenten og B-abonnenten er tilknyttet ulike tilbydere, må dermed A-abonnentens tilbyder av faktureringshensyn innhente navn- og adresseinformasjon om B-abonnenten hos B-abonnentens tilbyder.

2.2.1 Fasttelefoni

Analysen fra Teleplan i 2006 viser at nesten alle tilbyderne av fasttelefoni lagrer de data som datalagringsdirektivet krever. Som nevnt ovenfor, er det ikke gitt at alle data finnes hos tilbyder som A-abonnement er kunde hos. De tilbyderne som ikke lagrer dataene direktivet krever vil, med eksisterende infrastruktur, imidlertid ha mulighet til å hente ut dataene. Flere av de minste tilbyderne kjøper tjenesten fra grossist. Lagringstiden er varierende og det samme gjelder formater som benyttes for lagring av data.

2.2.2 Mobiltelefoni

De fleste tilbydere av mobiltelefonitjeneste lagrer i dag dataene som direktivet krever, med unntak av historisk knytning mellom celle-id og geografisk lokasjon. Som for fasttelefoni, er det ikke gitt at alle data finnes hos tilbyderen som A-abonnent er kunde hos. Tilbyder har altså kun navn og adresse til A-abonnement, ikke B- og C-abonnement med mindre de er kunde hos tilbyder. Det samme gjelder IMSI- og IMEI-nummer, hvor tilbyder kun har IMSI- og IMEI-nummer for samtaler originert i deres nett. IMSI står for International Mobile Subscriber Identity, og er et eget nummer for hver abonnement. Nummeret er unikt for hvert SIM-kort. Måten data lagres på er forskjellig hos de ulike tilbyderne av mobiltelefoni, og det er ikke uvanlig at data i tillegg lagres fragmentert i flere systemer hos hver tilbyder.

2.2.3 Internettaksess

Tilbydere av internettaksess lagrer bare i noen grad de data som direktivet forutsetter at skal lagres. I henhold til ekomloven § 2-7, kan tilbyderne kun lagre data som er nødvendige for fakturerings- og kommunikasjonsformål. Teleplans analyse viser at de aller fleste tilbyderne av internettaksess har mulighet til å kunne lagre de data som fremgår av direktivet, og vil med relativt enkle grep kunne hente ut de dataene som politiet etterspør. De fleste tilbyderne av internettaksess vil imidlertid måtte legge til rette for mer lagringsplass og etablere sikkerhetsrutiner og systemer for utlevering av data.

2.2.4 Bredbåndstelefoni

I korte trekk kan bredbåndstelefoni beskrives som at tale overføres elektronisk ved hjelp av internettprotokollene, og at tjenesten leveres over en bredbåndstilknytning. Bredbåndstelefoni tilbys i mange ulike varianter. De formene for bredbåndstelefoni som vil kunne omfattes av lagringsplikten kan sammenlignes med tradisjonell fasttelefoni, det vil i enkelhet si tjenester som er tilgjengelige for allmennheten og hvor telefonnummer etter nasjonal nummerplan benyttes. Basert på tilbakemeldinger fra enkelte tilbydere, er lagringsbehovet og tiden dataene lagres den samme som for fasttelefoni. Departementene er også kjent med at samtaler mellom to abonnenter/brukere hos samme tilbyder i noen tilfeller er gratis og at trafikkdata i slike tilfeller lagres i et meget kort tidsrom (timer). Også for bredbåndstelefoni ser departementene at enkelte tilbydere må gjennomføre endringer i lagringspraksis for å kunne tilfredsstille en eventuell lagringsplikt.

2.2.5 E-post

Når det gjelder e-post er det ulike måter å levere e-post på (direkte aksess, aksess via web-server og aksess via lokalnettoppsett). De ulike leveringsmåtene gir tilgang til ulik mengde og type data for tilbyderne. Praksis i dag er at noen tilbydere lagrer avsenders IP-adresse, avsenders og mottakers e-postadresse og tidspunkt for kommunikasjon. Det er ikke gitt at alle tilbyderne har alle disse dataene lett tilgjengelige. Teleplans utredning fra 2006 viser at det er under halvparten av tilbyderne som lagrer de data som direktivet krever. Dette bildet kan ha endret seg noe de siste par årene.

2.3 **Tilbyders taushetsplikt**

Ekomloven § 2-9 fastsetter taushetsplikten som gjelder ved bruk av elektronisk kommunikasjon.

Bestemmelsens første ledd fastslår at det gjelder taushetsplikt for innholdet av elektronisk kommunikasjon og andres bruk av elektronisk kommunikasjon, herunder tekniske innretninger og fremgangsmåter. Taushetsplikten gjelder for tilbyder av elektronisk kommunikasjonsnett- eller tjeneste. Det følger av andre ledd at taushetsplikten også gjelder for personer som utfører arbeid eller tjeneste for slik tilbyder og at taushetsplikten fortsetter å gjelde også etter at vedkommende har avsluttet arbeidet eller tjenesten.

Taushetsplikten etter første og andre ledd omfatter innholdet av kommunikasjonen. Videre omfatter taushetsplikten bruken av elektronisk kommunikasjon. Begrepet "bruk" knytter seg til alle sider av et abonnementsforhold for elektronisk kommunikasjon. For fast- og mobiltelefoni innebærer dette at alle opplysninger om inn- og utgående samtaler, det vil si hvilke telefonnumre som har vært satt i kontakt med hverandre, kommunikasjonens varighet og eventuelle basestasjoner som ble benyttet (lokaliseringsdata) er omfattet av taushetsplikten. Tilsvarende opplysninger knyttet til bruken av annen elektronisk kommunikasjon enn telefoni, herunder internettaksess,

bredbåndstelefoni og e-post, er omfattet. Utgangspunktet for opplysninger som omfattes av taushetsplikten etter § 2-9 første og andre ledd er at utlevering bare kan skje med hjemmel i lov.

Bestemmelsens tredje ledd oppstiller et viktig unntak for visse opplysninger, som knytter seg til identifikasjon og som kan utleveres til påtalemyndigheten og politiet uavhengig av taushetsplikten i første ledd. Unntaket ble i sin tid innført for å sikre politi og påtalemyndighet en enkel tilgang til identifikasjonsdata for personer med "hemmelig nummer". Bestemmelsens ordlyd er siden endret for å ta høyde for teknologiske utviklingstrekk, men omfatter fortsatt kun identifikasjonsdata, nærmere bestemt avtalebasert hemmelig telefonnummer og andre abonnementsopplysninger, samt elektronisk kommunikasjonsadresse. Etter § 2-9 fjerde ledd er tilbyder pålagt å etterkomme en anmodning fra påtalemyndigheten eller politiet om utlevering av slike identifikasjonsopplysninger, med mindre særlige forhold gjør det utilrådelig. Politiets tilgang etter denne bestemmelse er ikke begrenset til tilfelle der det skjer etterforskning av en straffesak. Politiets tilgang til andre typer data enn slike identifikasjonsopplysninger, må være hjemlet i straffeprosessloven (se kapittel 2.4).

2.4 **Politiets tilgang**

2.4.1 Sikringspålegg – straffeprosessloven § 215 a

Etter straffeprosessloven § 215 a kan påtalemyndigheten som ledd i etterforskningen gi pålegg om sikring av elektronisk lagrede data. Et sikringspålegg kan omfatte alle former for data, uten hensyn til om de er bærere av tall, symboler eller bokstaver, om disse i kombinasjon er meningsbærende og om dataene er kryptert. Bestemmelsen omfatter dermed både trafikkdata og innholdsdata, herunder filer med lyd, bilder eller tekst, jf. Ot.prp. nr. 40 (2004-2005) side 35.

Det er et grunnvilkår at sikringspålegget skjer som ledd i etterforskningen, samt at dataene "antas å ha betydning som bevis" i en straffesak, jf. § 215 a første ledd. Dette vilkåret skal tolkes på samme måte som det tilsvarende vilkåret i straffeprosessloven § 203 om beslag, jf punkt 2.4.2. Dersom pålegget retter seg mot en tilbyder av tilgang til elektronisk kommunikasjonsnett eller elektronisk kommunikasjonstjeneste, og gjelder innholdet av en elektronisk postsending eller et vedlegg til en slik sending, er det et tilleggsvilkår at det er "grunn til å tro at det er begått en straffbar handling".

Det er videre et vilkår at de aktuelle dataene allerede foreligger i elektronisk lagret form på det tidspunktet sikringspålegget utferdiges. Et sikringspålegg kan dermed ikke gis virkning fremover i tid, i motsetning til en beslutning om kommunikasjonskontroll, jf. straffeprosessloven §§ 216 a og 216 b. For øvrig gjelder pålegget for et bestemt tidsrom, som ikke må være lengre enn nødvendig, jf. fjerde ledd. Sikringsperioden kan høyst utgjøre 90 dager om gangen.

Endelig kommer hensiktsmessighetsprinsippet og forholdsmessighetsprinsippet i straffeprosessloven § 170 a til anvendelse. Den som treffer beslutningen om å bruke et tvangsmiddel, her sikringspålegg, må følgelig også vurdere om det er hensiktsmessig og ønskelig på avgjørelsestidspunktet, samt om det er forholdsmessig sett i forhold til sakens art og forholdene for øvrig.

Pålegget kan rette seg mot enhver som besitter slike data som ønskes sikret. Det fremgår av tredje ledd at en mistenkt skal gis underretning om beslutningen straks dataene er sikret og han får status som siktet i saken. Retter sikringspålegget seg mot en annen enn den mistenkte, skal underretning gis straks pålegget er gjennomført.

Sikringspålegget gir ikke automatisk rett for påtalemyndigheten til å få de sikrede dataene utlevert. Data som er sikret gjennom et sikringspålegg, kan i utgangspunktet bare kreves utlevert innenfor rammene av straffeprosessloven § 210, jf. Ot. prp. nr. 40 (2004-2005) punkt 4.2.4.3 side 28. Påtalemyndigheten har imidlertid etter begjæring tilgang til opplysninger som er nødvendige for å avdekke hvor de aktuelle dataene kom fra, og hvor de i tilfellet ble sendt til, jf. § 215 a siste ledd.

2.4.2 Beslag og utleveringspålegg – straffeprosessloven kapittel 16

Ting som kan ha betydning som bevis kan beslaglegges av påtalemyndigheten, eller retten kan pålegge besitteren å utlevere tingen, jf. straffeprosessloven §§ 203 og 210. Elektronisk lagrede data er å regne som "ting" etter disse bestemmelsene. Bruk av dette tvangsmidlet må dessuten oppfylle kravene i straffeprosessloven § 170 a, jf. punkt 2.4.1.

I praksis og juridisk teori er det lagt til grunn at sammenhengen mellom reglene om de forskjellige tvangsmidlene taler for at det også her må innfortolkes et krav om skjellig grunn til mistanke om en bestemt straffbar handling for å kunne foreta beslag, jf. Rt. 1998 side 1839 og 2000 s. 577 og Tor-Geir Myhrer : Andenæs Norsk straffeprosess 4. utg. (2009) på side 316. Videre må det være en rimelig mulighet for at de elektroniske dataene som ønskes beslaglagt eller utlevert kan kaste lys over spørsmålet om når, hvor, hvordan og/eller av hvem det er begått en straffbar handling. At en bestemt person skal være mistenkt, kreves derimot ikke, heller ikke at handlingen er av en viss grovhet.

Reglene om beslag- og utleveringspålegg er begrenset av reglene om vitneplikt, jf. § 204. I henhold til § 118 kan retten bare ta imot forklaring som et vitne kan gi uten å krenke lovbestemt taushetsplikt, jf. punktet om tilbyders taushetsplikt. Bevisforbudet etter straffeprosessloven § 118 gjelder imidlertid ikke ubetinget. Etter bestemmelsens første ledd første punktum kan departementet samtykke i at vitnet gis anledning til å forklare seg uten hinder av taushetsplikten. Samtykke kan bare nektes dersom forklaringen vil kunne utsette staten eller allmenne interesser for skade eller virke urimelig overfor den som har krav på hemmelighold, jf. annet punktum.

Samferdselsdepartementet har i vedtak 23. juni 1995 nr. 39 delegert kompetansen til Post- og teletilsynet. I praksis vil Post- og teletilsynets opphevelse av taushetsplikten føre til utlevering av de opplysningene som det ønskes forklaring om.

Utleveringspålegg avgjøres som hovedregel av retten, jf. straffeprosessloven § 210 første ledd, mens beslag besluttes av påtalemyndigheten dersom trafikkdataene ikke utleveres frivillig, jf. § 205 første ledd første punktum. For begge typer beslag er det egne regler om hastekompetanse, henholdsvis for politiet etter § 206 og for påtalemyndigheten etter § 210 annet ledd (fare ved opphold).

Det følger av straffeprosessloven § 205 første ledd siste punktum sammenholdt med § 208 a, at den saken gjelder – den som rammes – som hovedregel skal ha underretning før beslaget gjøres. Enhver som rammes av et beslag, har rett til å få dette prøvet av retten, jf. § 208. Det er mulighet for utsatt underretning (såkalt hemmelig beslag/utleveringspålegg). Vilkårene er at noen med skjellig grunn mistenkes for en handling eller forsøk på handling med en strafferamme på mer enn 6 måneder og at utsatt underretning er strengt nødvendig av hensyn til etterforskningen, jf. §§ 210 a og 208 a. Når retten behandler en sak etter § 208 a og 210 a, skal det straks oppnevnes offentlig advokat for den mistenkte, jf. straffeprosessloven § 100 a.

2.4.3 Kommunikasjonskontroll – straffeprosessloven kapittel 16

Straffeprosessloven §§ 216 a og 216 b gir hjemmel for politiet til å gjennomføre henholdsvis kommunikasjonsavlytting og annen kommunikasjonskontroll. Kommunikasjonsavlytting kan innebære avlytting av telefonsamtaler eller lesing av tekstmeldinger eller e-poster. Kommunikasjonskontroll kan for eksempel gå ut på å stenge et anlegg for kommunikasjon eller gi politiet opplysninger om hvilke kommunikasjonsanlegg som har vært i forbindelse med hverandre. Et grunnvilkår for begge typer kommunikasjonskontroll er at retten ved kjennelse har besluttet slik kontroll. I straffeprosessloven § 216 d er det likevel åpnet for at påtalemyndigheten i saker hvor det haster, kan beslutte kommunikasjonskontroll. Beslutningen må imidlertid legges frem for retten innen 24 timer etter at kontrollen ble påbegynt.

Et annet grunnvilkår for å foreta kommunikasjonskontroll er at det foreligger skjellig grunn til mistanke om en straffbar handling med strafferamme på 10 år (kommunikasjonsavlytting etter straffeprosessloven § 216 a) eller 5 år (kommunikasjonskontroll etter straffeprosessloven § 216 b), eller at den straffbare handlingen rammes av nærmere angitte straffebestemmelser. Mindre strenge vilkår for å foreta annen kommunikasjonskontroll, avspeiler at dette tvangsmidlet regnes som mindre inngripende enn kommunikasjonsavlytting. Mistanken må dessuten rette seg mot en bestemt person.

Tvangsmidler som nevnt i straffeprosessloven kapittel 16 a kan således bare benyttes for å etterforske saker om lovbrudd av en viss grovhet, samt i saker der en antar kommunikasjonskontroll vil være en særlig effektiv etterforskningsmetode. I tilegg gjelder det et krav om at metodebruken må være av vesentlig betydning for å oppklare saken, og at oppklaringen ellers i vesentlig grad vil bli vanskeliggjort, jf. § 216 c. Endelig vil også straffeprosessloven § 170 a om hensiktsmessighetsprinsippet og forholdsmessighetsprinsippet komme til anvendelse også ved bruk av slike tvangsmidler.

Retten treffer beslutningen om kommunikasjonskontroll uten at den mistenkte eller den avgjørelsen rammer, gis adgang til å uttale seg. Kjennelsen blir heller ikke meddelt vedkommende, jf. straffeprosessloven § 216 e annet ledd. Når det er gått ett år eller mer etter at kontrollen er avsluttet, kan imidlertid enhver som ber om det – med enkelte unntak – gis underretning om hvorvidt vedkommende har vært underlagt kommunikasjonskontroll, jf. straffeprosessloven § 216 j. Kontrollutvalget for kommunikasjonskontroll skal føre kontroll med all kommunikasjonskontroll som foretas i medhold av kapittel 16 a om kommunikasjonskontroll, jf. straffeprosessloven § 216 h. Det gjelder likevel ikke for saker som omfattes av lov om kontroll med etterretnings-, overvåknings- og sikkerhetstjeneste. Kontrollutvalget er forutsatt særlig å skulle ivareta mistenktes og andre berørtes interesser.

En nødvendighetsgrense for tillatelse til kommunikasjonskontroll er nedfelt i straffeprosessloven § 216 f som foreskriver at slik tillatelse normalt bare kan gis for 4 uker om gangen. Informasjon som viser seg å være uten betydning skal slettes, jf. § 216 g.

2.4.4 Metodekontrollutvalgets utredning NOU 2009: 15

Kongen i statsråd nedsatte 15. februar 2008 et utvalg for å foreta en etterkontroll av reglene om nye etterforskningsmetoder for å styrke kampen mot alvorlig kriminalitet. Utvalget, heretter omtalt som Metodekontrollutvalget, avleverte sin utredning 26. juni 2009 som NOU 2009: 15 "Skjult informasjon – åpen kontroll". Utredningen er tilgjengelig på www.regjeringen.no/jd

Utvalget har her bl.a. vurdert reglene for politiets innhenting av trafikkdata. De uttaler i utredningen punkt 2.10 på side 26:

"I dag er den enkelte teletilbyders praksis avgjørende for hvilke krav som stilles til politiets beslutning om å innhente trafikkdata. Dette kan enten skje ved at teletilbyder utleverer opplysningene frivillig, etter beslutning fra Post- og teletilsynet om å oppheve tilbyders taushetsplikt, etter beslutning om beslag eller utleveringspålegg, eventuelt etter straffeprosessloven § 216b. Denne situasjonen er etter utvalgets oppfatning lite tilfredsstillende, og det foreslås derfor at innhenting bare skal kunne skje etter beslutning om utleveringspålegg fattet av retten, eventuelt i kombinasjon med utsatt underretning om dette. Fordi Post- og teletilsynet som regel vil ha mangelfull tilgang til faktum i saken og fordi tilsynets vurdering ikke anses nødvendig når utlevering etter utvalgets forslag uansett skal besluttes av domstolen,

foreslås at Post- og teletilsynet fratas denne oppgaven. Dette foreslås gjort ved at trafikkdata unntas fra tilbyders taushetsplikt etter ekomloven § 2–9 dersom det foreligger beslutning om utleveringspålegg."

I den forbindelse tar utvalget også opp problemer knyttet til manglende straffesanksjonering av tilbyders brudd på taushetsplikten vedrørende informasjon om utlevering av trafikkdata til politiet. De uttaler i utredningen punkt 20.5 på side 221:

"Det understrekes at politiet fremdeles vil kunne pålegge teletilbyderne taushetsplikt med hjemmel i straffeprosessloven § 61c siste ledd første punktum. Overtredelse av slike pålegg kan straffes etter straffeloven § 121, så fremt vedkommende er gjort oppmerksom på dette, jf. § straffeprosessloven 61c siste ledd siste punktum. Utvalget er imidlertid blitt gjort oppmerksom på at det ikke finnes en tilsvarende hjemmel til å pålegge taushetsplikt om skjult tvangsmiddelbruk etter politiloven. Selv om «alle» vil ha taushetsplikt om dette etter politiloven § 17d, jf. § 17f, er overtredelse av slik taushetsplikt ikke straffbart for personer som ikke i utgangspunktet rammes av straffeloven § 121. Teletilbydere som bryter denne taushetsplikten kan dermed ikke straffes, noe som ifølge PST har medført problemer. Etter utvalgets oppfatning er det ingenting som tilsier at brudd på taushetsplikten etter § 17f ikke bør få samme konsekvenser for alle involverte, og utvalget foreslår derfor at det tas inn en henvisning i politiloven § 17f til straffeloven § 121 lik den som finnes i straffeprosessloven § 61c siste ledd siste punktum."

På denne bakgrunn foreslo utvalget følgende utforming av politiloven § 17f:

"Alle skal bevare taushet om at det er begjært eller besluttet bruk av tvangsmidler etter § 17 d, og om opplysninger som fremkommer ved bruk av tvangsmidlet. Det samme gjelder andre opplysninger som er av betydning for forebygging eller etterforsking, og som man blir kjent med i forbindelse med bruken av tvangsmidlet eller saken.

Taushetsplikten er ikke til hinder for at opplysningene brukes

1. som ledd i å forebygge et straffbart forhold som nevnt i § 17 b første ledd,
2. som ledd i etterforsking av et straffbart forhold som nevnt i § 17 d første ledd, herunder som ledd i avhør av de mistenkte,
3. som bevis for en terrorhandling, jf. straffeloven § 147 a *første og annet ledd,*
4. for å forebygge at noen uskyldig blir straffet, eller
5. for å forhindre en alvorlig straffbar handling som kan krenke andres liv, helse eller frihet.

Overtredelse av taushetsplikt etter denne bestemmelsen kan straffes etter straffeloven § 121. Dette gjelder også for personer som ikke er i tjeneste eller arbeid for statlig eller kommunalt organ, dersom vedkommende er gjort oppmerksom på at overtredelsen kan få slik følge."

Forslaget til nytt tredje ledd kommenteres slik i utredningen punkt 31.2 på side 363:

"Utvalget foreslår også en presisering av at brudd på taushetsplikten etter bestemmelsen kan straffes etter straffeloven § 121, og at dette også gjelder personer som ikke er i tjeneste eller arbeid for statlig eller kommunalt organ. Også personer utenfor politiet eller påtalemyndigheten som får kjennskap til tvangsmiddelbruken, for eksempel ansatte hos teletilbyderne, vil dermed kunne straffes for brudd på taushetsplikten. Utenforstående bør

imidlertid gjøres oppmerksom på denne muligheten, jf. også straffeprosessloven § 61c siste ledd siste punktum."

Justisdepartementet sendte Metodekontrollutvalgets utredning på høring 15. desember 2009. Høringsfristen er satt til 1. mai 2010. De problemstillinger som utvalget tar opp i kapittel 20 om innhenting av trafikkdata vil imidlertid i hovedsak bli fulgt opp i forbindelse med eventuelle lovendringer for å gjennomføre datalagringsdirektivet i norsk rett.

2.5 **Praksis for utlevering av trafikkdata fra tilbyderne til politiet**

For at tilbyder skal kunne utlevere historiske trafikkdata som er underlagt taushetsplikt etter ekomloven § 2-9, må Post- og teletilsynet først ha gitt sitt samtykke til utlevering etter straffeprosessloven § 118 første ledd. Politiet må derfor rette en anmodning til Post- og teletilsynet der de ber om fritak fra taushetsplikten i den konkrete saken. Etter straffeprosessloven § 118 første ledd siste punktum kan samtykke bare nektes dersom *" åpenbaringen vil kunne utsette staten eller allmenne interesser for skade eller virke urimelig overfor den som har krav på hemmelighold".*

Post- og teletilsynet foretar på denne bakgrunn en konkret rimelighetsvurdering tilsvarende prinsippene i straffeprosessloven § 170a. Der anmodningen gjelder trafikkdata fra mobil- eller fasttelefon legger Post- og teletilsynet vekt på hvorvidt telefonen disponeres av en person som har straffeprosessuell stilling som siktet eller mistenkt for et konkret straffbart forhold. På bakgrunn av personvernhensyn er tilsynet svært restriktive med å gi fritak for taushetsplikt der trafikkdata kan knyttes til en person som ikke er siktet eller mistenkt for et straffbart forhold. Bakgrunnen for dette er at trafikkdata kan gi mye informasjon om en persons bevegelses- og atferdsmønster. Videre legger Post- og teletilsynet vekt på om det er innledet etterforskning av et straffbart forhold, og hvor viktig elektroniske spor er for etterforskning av saken. Når det gjelder anmodning om basestasjonsøk, foretar Post- og teletilsynet en vurdering av befolkningstetthet i det geografiske området det anmodes trafikkdata fra, det straffbare forholds alvorlighet og karakter, varigheten av det omsøkte basestasjonsøket, samt hvilken tid på døgnet begjæringen knytter seg til.

Dersom Post- og teletilsynet sier nei til å frita fra taushetsplikten, kan spørsmålet overprøves av retten etter straffeprosessloven § 210 jf. § 118 annet ledd.
Når det gjelder utlevering av abonnentsopplysninger, kan politiet henvende seg direkte til tilbyder uten å innhente forutgående samtykke fra Post- og teletilsynet, jf ekomloven § 2-9 tredje ledd.

Ifølge Post- og teletilsynet, har Telenor (konsern), NetCom, Tele2, Ventelo (konsern) og Network Norway blitt enige om å kreve beslutning om beslag i tillegg til fritak fra Post- og teletilsynet når det gjelder utlevering av trafikkdata til politiet. Politiet forholder seg i praksis utelukkende til Telenor eller NetCom i forbindelse med utlevering av

trafikkdata. Årsaken til dette er at det i all hovedsak har vært Telenor og NetCom som har eget mobilnett og Telenor som har fastnett. Videreselgere, som for eksempel Chess, leier nettjenester fra enten Telenor eller NetCom og lagrer trafikkdata om egne kunder kun til bruk for deres fakturering av sluttkundene. Disse trafikkdataene lagres i tillegg hos Telenor eller NetCom fordi disse danner grunnlag for fakturering av underleverandøren (samtrafikkavregning).

Det har vært reist spørsmål om utlevering av trafikkdata kan skje i forbindelse med et politiavhør som ledd i vitneforklaring etter straffeprosessloven § 230, eventuelt rettslig avhør etter straffeprosessloven § 237. Til støtte for en slik forståelse av vitneplikten har det blitt anført at det i stedet for samtykke til vitneforklaring, må kunne gis samtykke til utlevering av dokumenter som inneholder de opplysningene som det ønskes forklaring om, jf Rt. 1930 side 1027. Det kan imidlertid anføres at den teknologiske utviklingen trolig har gjort det mindre naturlig å anse tilbyders utlevering av trafikkinformasjon som et vitnebevis, fordi det som i dag utleveres er utskrifter/lister med til dels store mengder data. Det er disse listene med informasjon som er det sentrale beviset for politiet.

Politiets innhenting av trafikkdata fra tilbyderne har økt kraftig de siste årene i takt med den teknologiske utviklingen. Tall innhentet fra Post- og teletilsynet viser dog at antallet begjæringer har holdt seg relativt stabilt de siste fem årene. Disse tallene reflekterer imidlertid ikke at den enkelte begjæring har blitt mer omfattende i den betydning at den enkelte begjæring inneholder begjæring om fritak fra taushetsplikten for flere telefonnumre. Videre opplyser Post- og teletilsynet at omfanget av begjæringer om fritak fra taushetsplikten for å kunne utføre basestasjonssøk har blitt mer omfattende, både i omfang og i varighet.

Post- og teletilsynet opplyser at de har mottatt følgende antall begjæringer de senere år:

2001: 982
2002: 1418
2003: 1597
2004: 1905
2005: 1961
2006: 1928
2007: 1976
2008: 1900

Tallene for 2009 ligger hittil i år på samme nivå som for 2008.

Departementene har bedt tilsynet om utdypende opplysninger om de anmodningene fra politiet om å frita tilbydere fra taushetsplikten som Post- og teletilsynet har behandlet tilbake fra 1. januar 2006. Tilsynet har opplyst at det ikke føres statistikk over innholdet av anmodningene fra politiet, eller utfallet av tilsynets behandling av disse saker. Opplysningene som har fremkommet er derfor basert på de erfaringer som tilsynet har opparbeidet, og er ikke eksakte tall eller fakta.

Post- og teletilsynet har opplyst at de anser hovedtyngden av begjæringene fra politiet til å gjelde mistanke om overtredelse av straffeloven § 162 (narkotika), § 257, evt. jfr. § 258 (tyveri/grovt tyveri) samt voldslovbrudd. Dataene gjelder nesten utelukkende mobiltelefoner. Det lagres i dag bare i mindre grad data om internettbruk og bredbåndstelefoni. Politiet opplyser at de derfor heller ikke etterspør slike data. Det vises også til at politiet har opplyst at det den senere tid har vært vanskeligere å etterforske internettrelaterte saker vedrørende overgrep mot barn. Dette skyldes blant annet at tilbyderne i dag ikke har rettslig grunnlag for å oppbevare data lenger enn tre uker, som er den tiden dataene anses nødvendige for kommersielle formål.

Post- og teletilsynet uttaler at de av eget tiltak innhenter tilleggsopplysninger dersom begjæringen inneholder for få opplysninger til at den kan behandles. Det anslås etter det opplyste at 10-15 % av begjæringene ikke blir tatt til følge (i 2008 ble 180 av 1800 ikke tatt til følge, hittil i 2009 er tallet ca. 200 av 1860 begjæringer). Hovedsakelig er årsaken til tilsynets avslag på fritak fra taushetsplikt at den som dataene gjelder ikke har status som mistenkt eller er siktet etter straffeprosessloven. Det kan også forekomme tilfelle der politiet ikke har innledet etterforskning av et straffbart forhold eller at politiet ikke har sannsynliggjort at de aktuelle data faktisk gjelder den som er mistenkt eller siktet i saken. Tilsynet gir i hovedsak fritak fra taushetsplikten for den periode politiet anmoder om og i de fleste tilfelle vil dette vær periode så langt tilbake i tid som trafikkdata er lagret, dvs. 3 måneder for Telenor og 5 måneder for NetCom. Andelen av begjæringer som gjelder basestasjonssøk (innhenting av trafikkdata fra basestasjoner 'en bloc') anslås i følge tilsynet å ligge på 8-10 %, men tilsynets anslag har et usikkert grunnlag. Tilsynet opplyser at dersom politiet kan avgrense tidsperiode og geografisk tilstrekkelig, blir begjæringer om fritak knyttet til basestasjonsøk i hovedsak etterkommet. For øvrig opplyser Post- og teletilsynet at politiet etter det tilsynet erfarer "i noen grad" benytter adgangen i straffeprosessloven § 215a til å sikre seg at trafikkdata ikke slettes, dvs. bevissikring. At politiet har benyttet bevissikring, fremgår imidlertid sjelden av begjæringene som Post- og teletilsynet mottar.

2.6 Andre myndigheters tilgang til trafikkdata i dag

Andre offentlige myndigheter enn politi og påtalemyndighet kan bare innhente opplysninger fra tilbyder om lagrede data dersom det finnes lovhjemmel som gjør unntak fra taushetspliktbestemmelsen i ekomlovens § 2-9. Innhentingen skjer da ikke som ledd i en straffesak. Det er et tiltak administrative myndigheter har rett til å foreta som et ledd i sin alminnelige kontroll med at lovgivningen på et bestemt område blir overholdt.

Et eksempel på slik hjemmel etter gjeldende regelverk er verdipapirhandelsloven § 15-3 annet ledd (2) og (3), som blant annet inneholder hjemmel for Kredittilsynet til å innhente opplysninger om trafikkdata etter Post- og teletilsynets forutgående opphevelse av tilbyders taushetsplikt. Denne lovbestemmelse følger samme systematikk som straffeprosessloven § 118, første ledd og tvisteloven § 22-3, der det forutsettes en forutgående opphevelse av taushetsplikten før den taushetsbelagte

informasjonen kan legges frem for domstolene. Ved vurderingen av om taushetsplikten skal oppheves skal det etter ordlyden i verdipapirhandelsloven § 15-3 annet ledd (3) blant annet legges vekt på hensynet til taushetsplikten og sakens opplysning. Primo 2008 sendte Finansdepartementet et forslag til forskrift om nærmere saksbehandlingsregler for Kredittilsynets innhenting av trafikkdata på høring. Forskriften er per 18. desember 2009 ikke trådt i kraft, og etter det departementene har fått opplyst finnes det per i dag ikke tilfeller der Post- og teletilsynet har fritatt tilbyder fra taushetsplikten på bakgrunn av at Kredittilsynet har bedt om å få hente ut trafikkdata.

3. RETTSTILSTANDEN OG IMPLEMENTERING AV DATALAGRINGSDIREKTIVET I ANDRE EUROPEISKE LAND

3.1 Danmark

Datalagringsdirektivet er i Danmark fullt ut implementert ved den såkalte "logningsbekendtgørelsen". Tilbydere av elektronisk kommunikasjonsnett eller -tjenester har i henhold til bekendtgørelse nr. 988 af 28/09/2006 om udbydere af elektroniske kommunikationsnets og elektroniske kommunikationstjenesters registrering og opbevaring af oplysninger om teletrafik (logningsbekendtgørelsen) plikt til å registrere og oppbevare opplysninger om teletrafikk i ett år (§ 9). Denne bekendtgjørelsen trådde i kraft 15. september 2007.

Politiets adgang til å hente ut data fremkommet ved bruk av elektronisk kommunikasjon er nedfelt i den danske retsplejeloven kapittel 71. Slike data kan bare kreves utlevert dersom det er bestemte grunner til å anta at den mistenkte bruker de kommunikasjonsmidler som utleveringsbegjæringen gjelder og utleveringen antas å være av avgjørende betydning for etterforskningen (§ 781). Dessuten må etterforskningen gjelde lovbrudd med en strafferamme på minst 6 år, eller forhold som rammes av nærmere opplistede straffebud, herunder handlinger mot rikets sikkerhet og statsforfatning, terrorisme, barnepornografi, samt visse brudd på utlendingsloven m.m. For at det skal kunne kreves utlevert data som knytter seg til et bestemt geografisk område, må mistanken i tillegg knytte seg til et straffbart forhold som medfører fare for liv og helse, eller betydelige samfunnsverdier. Endelig skal utlevering av data bare kunne foretas såfremt det i lys av formålet, sakens betydning, og ulempene for de det gjelder, ikke er et uforholdsmessig tiltak (§ 782).

Utlevering skal som hovedregel bare skje etter forutgående avgjørelse av domstolen (§ 783). Unntak herfra gjelder dersom saken haster. I så fall skal politiet snarest og senest innen 24 timer fra data er begjært utlevert, forelegge saken for retten. Før retten treffer en avgjørelse i saken, skal det oppnevnes advokat for den som utleveringen av data gjelder (§ 784).

Etter at data er utlevert, skal den eller de som dataene knytter seg til, underrettes om dette (§ 788). Unntak herfra gjelder dersom slik underretning kan være til skade for etterforskningen. Underrettelsesplikten gjelder heller ikke for data som knytter seg til et bestemt geografisk område.

Overskuddsinformasjon kan brukes av politiet i etterforskningsøyemed (§ 789). Informasjonen kan imidlertid som hovedregel ikke brukes som bevis i en annen sak enn den som utleveringen knyttet seg til.

Det er tilbyderne som dekker investeringskostnadene knyttet til lagringsplikten, mens myndighetene betaler for uthenting av data. Den danske ekombransjen har beregnet at kostnaden forbundet med lagring er i størrelsesorden 100-200 millioner danske kroner dersom alle data lagres i 12 mnd. I tilegg kommer kostnader til uthenting. En stor del av kostnadene er knyttet til lagring av internettrelaterte data.

Departementene har for øvrig fått opplyst at danske myndigheter har satt ned en arbeidsgruppe som blant annet skal se på registrering av brukere av forhåndsbetalte tjenester, internettkafeer, gratis trådløs sone (wlan) og Internett på biblioteker.

3.2 **Finland**

Datalagringsdirektivet har blitt gjennomført i finsk rett gjennom endringer i lag om dataskydd vid elektronisk kommunikation 16.6.2004/516. Lovendringen trådte i kraft 1. juni 2008. Av lagen 14 a § følger at data skal lagres i ett år.

Endringen medførte en prinsipiell endring i loven. Fra å pålegge tilbydere å lagre for forretningsmessige formål, skal data nå også lagres for å dekke myndighetenes behov. Hva som skal lagres fremgår av forskrift av 5. juni 2008 om plikt til å lagre identifikasjonsdata.

Myndighetene kan begjære utlevering av data kun i etterforskningsøyemed og såfremt vilkårene i 5 a kap. 3 § 1 i tvångsmedelslagen (450/1987) er oppfylt. Denne bestemmelsen omhandler vilkårene for kommunikasjonskontroll. Slik kontroll kan begjæres blant annet dersom det foreligger skjellig grunn til mistanke om en lovovertredelse som har minst fire års strafferamme, eller dersom forholdet gjelder datakriminalitet, hallikvirksomhet, trusler, narkotikaforbrytelser eller terrorvirksomhet.

Det fremgår av kapittel 98 i lov om kommunikasjonsmarkedet (Communications Market Act) at de merkostnadene som lagringsplikten påfører tilbyderne, skal dekkes av den myndighet i hvis interesse lagringen skjer, dvs. justismyndighetene (Inrikesministeriet).

3.3 **Sverige**

Sverige har per i dag ingen plikt for tilbydere av elektronisk kommunikasjonsnett og -tjenester til å lagre data. Datalagringsdirektivet er ikke gjennomført i svensk lov og EU-kommisjonen har på bakgrunn av dette trukket Sverige inn for EF-domstolen. Svenske myndigheter satte i 2006 i gang en utredning som har sett på hvordan EUs datalagringsdirektiv kan implementeres i svensk rett. Denne ble avgitt i november 2007 (SOU 2007: 76). Utredningen ble sendt på høring våren 2008 og det svenske justitiedepartementet arbeider nå med å følge opp saken. I utredningen anbefaler utvalget at svenske myndigheter innfører en lagringsplikt der tilbyder selv skal kunne velge lagringsløsning. Lagringstiden foreslås til ett år. Tilbyderne skal dekke kostnader knyttet til tilrettelegging og lagring, mens Politiet skal dekke kostnader knyttet til uthenting av trafikkdata. Inkludert i uthentingskostnadene regnes utgifter til tekniske system, samt drift og vedlikehold av systemene. Det samme gjør personellkostnader og kostnader knyttet til å finne grensesnittet opp mot politiets systemer.

I svensk rett er det allerede i dag adgang til å få ut data. I kapitlet om hemlig teleövervakning i rättegångsbalken kan utlevering av data gis etter beslutning av retten. Det kan bare gis dersom det er mistanke om lovbrudd med minst 6 måneders strafferamme, datakriminalitet, grovere tilfeller av barnepornografi eller narkotikaforbrytelser. Dessuten kan utlevering av data også skje med hjemmel i lagen om elektronisk kommunikation. Slik utlevering kan skje etter begjæring fra påtalemyndighetene, men må til gjengjeld knytte seg til overtredelser av straffebestemmelser med minst 2 års strafferamme. Lagen om elektronisk kommunikation har også særskilte regler om utlevering av abonnementsopplysninger. Det gjelder ikke like strenge krav for utlevering av slike opplysninger. På nærmere angitte vilkår kan dessuten også Kronofogdemyndigheten og Skatteetaten få tilgang på disse.

Mye tyder på at saken om datalagringsdirektivet vil ta lengre tid enn først antatt i Sverige. Personverndebatten har vært omfattende som følge av den nylig innførte FRA-loven, som gir svensk etterretningstjeneste adgang til å spane på alle signaler som krysser Sveriges grenser i kabel, Pirat-Bay saken og datalagringsdirektivet. Norske myndigheter er ikke kjent med om og når et lovforslag om implementering av datalagringsdirektivet skal legges frem for Riksdagen.

3.4 **Andre EU-land**

Alle EUs medlemsstater har gjennomført datalagringsdirektivet i nasjonal lovgivning med unntak av Sverige, Irland, Hellas og Østerrike. Den største gruppen av medlemsstater med samme lagringstid for alle typer data har innført 12 måneders lagringstid. I de fleste statene er det nødvendig med en tillatelse fra retten for å få utlevert data. Departementene er imidlertid kjent med at det har vært reist spørsmål til gjennomføringen av direktivet i nasjonal rett i Romania, Tyskland og Ungarn. Den rumenske konstitusjonsdomstolen nylig har avsagt en dom hvor de finner at den rumenske loven som gjennomfører datalagringsdirektivet, er i strid med individets rettigheter slik disse er nedfelt i den rumenske grunnloven. De aktuelle bestemmelsene

i grunnloven bygger bl.a. på Den europeiske menneskerettighetskonvensjonen (EMK) artikkel 8. I sin begrunnelse viser domstolen til at en slik konsekvent og systematisk lagring av data er for vidtgående og undergraver hovedregelen om retten til privatliv. De to andre sakene er foreløpig uavklarte.

EU-kommisjonen har gått til sak mot Hellas, Sverige, Østerrike, Irland, Polen og Nederland for manglende gjennomføring av direktivet i nasjonal rett. Polen og Nederland har imidlertid gjennomført direktivet i nasjonal rett etter at prosessen om manglende gjennomføring ble iverksatt. I to dommer avsagt 26. november 2009 av EU-domstolen ble henholdsvis Hellas (saksnr. 211/09) og Irland (saksnr. 202/09) dømt for manglende gjennomføring av direktivet. Etter det en har fått opplyst fra greske myndigheter, er treghet i statsadministrasjonen den viktigste årsaken til forsinkelsen. EF-domstolen har ennå ikke tatt stilling til saken mot Sverige og Østerrike.

4. NÆRMERE OM LOVFORSLAGET

4.1 Ulike hensyn som må avveies

Det er i hovedsak tre hensyn som må vurderes og avveies ved innføring av en plikt om datalagring. Det første hensynet er behovet for verktøy til å bekjempe kriminalitet.

Politiet skal i henhold til politiloven § 1 "gjennom forebyggende, håndhevende og hjelpende virksomhet være et ledd i samfunnets innsats for å fremme og befeste borgernes rettsikkerhet, trygghet og alminnelige velferd for øvrig". Politiet utfører sine oppgaver på vegne av staten som "skal sørge for den polititjeneste som samfunnet har behov for".

Målet for politiets virksomhet er i politiinstruksen formulert som "å opprettholde den offentlige orden og sikkerhet, forfølge lovbrudd og utføre andre oppgaver fastsatt etter lov eller sedvane. I ethvert tilfelle gjør politiet best nytte for seg hvis det på forhånd lykkes i å forebygge eller avverge lovbrudd eller ordensforstyrrelser.

Effekten av politiets innsats er å tilfredsstille borgernes behov for rettssikkerhet, trygghet og alminnelig velferd. Dette er tre grunnleggende samfunnsbehov av allmenn karakter. For å kunne løse disse oppgavene til beste for samfunnet er politiet tillagt metoder og virkemidler. Politiets arbeidsmetoder og virkemidler for å kartlegge, avdekke og stanse kriminell virksomhet er mange. Metodene avhenger av på hvilket stadium i handlingsrekken det dreier seg om. Dette er alt fra informasjonsarbeid til lovregulert romavlytting.

Teknologiaspektet er mangeartet, men vel så viktig som at teknologien gir kriminelle nye muligheter til å kommunisere med hverandre i planleggingen av nye straffbare handlinger, øker farene for internasjonal organisering av forbrytelsene.
Dataene i henhold til datalagringsdirektivet er opplysninger som i seg selv vil kunne ha stor bevisverdi i straffesaker (typisk når, hvor og hvem som foretok en oppringning).

Særlig ved alvorlig og organisert kriminalitet der elektronisk kommunikasjon har blitt benyttet under planlegging og gjennomføring av straffbare handlinger, vil trafikkdata, lokaliseringsdata og abonnements/brukerdata være viktige for politi og påtalemyndighet som bevis i saken. I enkelte typer straffesaker vil denne type data også kunne fremstå som avgjørende bevis, det kan for eksempel være tilfelle ved ulovlig distribusjon eller nedlasting av materiale som viser seksuelle overgrep mot barn på Internett. Data kan utgjøre de støttepunkter en forklaring behøver for å bli lagt til grunn i domstolene. Påfølgende beslag som politiet kan foreta som følge av at de har fått data, kan få enda større betydning (beslag i datamaskin som avdekker ulovlig elektronisk materiale og et større kriminelt nettverk).

Tilgang til data er nødvendigvis ikke bare av interesse for politiet. Fornærmede har et menneskerettslig krav på vern mot overgrep fra andre borgere. Dette påkrever ofte at landets myndigheter har tilstrekkelige effektive redskaper til å strafforfølge slike overgrep. Siktedes legitime interesse er at straffesaken blir avgjort på et materielt riktig grunnlag. At data, og eventuelt senere innhentet innhold, godtgjør omstendigheter som betyr at det påståtte straffbare forhold ikke kan legges til grunn som tilstrekkelig bevist, er på det rene. At politiet får lettere tilgang til data, vil kunne føre til at flere kriminelle blir "tatt". Bedre opplysning av straffesakene vil også kunne føre til at antallet og andelen uriktige domfellelser går ned. Politiets tilgang til data er også viktig for å hindre gjennomføringen av organisert kriminalitet og avverge forberedelser til terroranslag. Innføringen av direktivet har således også en kriminalitetsforebyggende virkning.

Det er særlig i bekjempelsen av den alvorlige kriminaliteten hvor det er viktig å sikre elektroniske spor som begrunner behovet. Etterforskningen er i slike saker ofte mer kompleks og har i tillegg ofte internasjonale dimensjoner. Politiets tilgang har betydning for å få saken så godt opplyst som mulig. Dagens strenge sletteregler kan komme i konflikt med fornærmedes krav på effektiv beskyttelse mot overgrep fra andre borgere, dersom myndighetene er forhindret fra å strafforfølge overgrepene pga. snever tilgang til nødvendige data. Kort slettefrist kan også komme i konflikt med siktedes rett til effektivt forsvar. Dersom siktede ikke har hatt anledning til å forberede sitt forsvar før politiet er i sluttfasen av en etterforskning hvor man ikke har innhentet data, kan bevismateriale i data som taler for siktedes uskyld ha gått tapt. Det kan også være viktig å etterforske en person ut av saken på et tidlig stadium, både for politiet og for personen selv.

Politiets tilgang til data vil derfor i mange tilfeller kunne være helt avgjørende for å kunne ivareta de oppgaver som etaten er tillagt i politiloven. Det vises også til de eksempler som begrunner lagringstid som er gjengitt i kapittel. 4.8.

Det andre hensynet er personvern. Lovpålagt lagringsplikt har vært diskutert en rekke ganger bl.a. i forbindelse med vedtagelse av ekomloven av 4.7.2003 og i forbindelse med NOU 2004:6 *Mellom effektivitet og personvern*. Datatilsynet og personvernorganisasjoner har vært sterkt i mot en lagringsplikt i norsk rett. Tilsvarende har personvernorganisasjoner i Europa vært imot europeisk lagring.

Personvernorganisasjonenes hovedinnvending mot innføring av datalagring i Europa er at plikten kan bidra til å redusere det vern av personlig integritet som er en del av rettsstatens rammer, og som blant annet er forankret i EMK og personvernlovgivningen. På europeisk nivå er det med utgangspunkt i artikkel 29 i direktiv 95/46/EF (personverndirektivet) etablert en rådgivende arbeidsgruppe for databeskyttelse og personvern (artikkel 29 gruppen). Denne gruppen har utarbeidet en egen uttalelse (opinion) om datalagring. Denne uttalelsen er å finne på http://www.regjeringen.no/nb/dep/fad/dok/nouer/2009/nou-2009-1/24.html?id=542291

Personvernhensyn, som alle andre grunnleggende rettigheter, må avveies og finne sitt innhold bla. i møte med andre viktige samfunnshensyn, herunder hensynet til kriminalitetsbekjempelse. Spørsmålet er om en lagringsplikt kan forsvares ut fra de hensyn som en slik plikt er ment å ivareta, nemlig hensynet til kriminalitetsbekjempelse.

Personvern beskrives ofte som et knippe interesser, både individuelle og kollektive. De individuelle personverninteressene bygger på tanken om at alle borgere har grunnleggende interesse i diskresjon ved behandling av personopplysninger, i at opplysninger som behandles er fullstendige og relevante, i innsyn i behandlingen og i privatlivets fred. De kollektive personverninteressene kan uttrykkes ved samfunnets ønsker om en borgervennlig forvaltning, et robust samfunn og et begrenset overvåkingsnivå. Dette siste hensynet er blitt stadig viktigere de senere årene, som følge av tiltagende registrering, overvåking og kontroll. Interessen i et begrenset overvåkingsnivå dreier seg om behovet for vern mot maktmisbruk og urimelig kontroll, både fra det offentlige og fra private aktører. Når man skal vurdere samfunnets overvåkingsnivå, må man vurdere det totale bildet, det vil si effekten av den samlede registreringen og kontrollen borgerne utsettes for.

Personvernlovgivningen har som uttalt formål å beskytte den enkelte mot at personvernet blir krenket gjennom behandling av personopplysninger. Dette skal blant annet skje gjennom å ivareta borgernes behov for personlig integritet og privatlivets fred, jf personopplysningsloven § 1. Registrering av alle borgeres elektroniske kommunikasjon vil over tid gi et svært godt bilde av deres kontaktnett og bevegelser. Dette inngrepet i kommunikasjonsfriheten og det ubehaget borgerne kan føle ved å vite at noen sitter med denne informasjonen, er i seg selv en integritetskrenkelse. Denne forsterkes ytterligere av de registrertes frykt for at informasjonen kan misbrukes eller komme uvedkommende i hende.

Et viktig element i personvernet er, som ovenfor nevnt, at samfunnets overvåkings- og kontrollnivå skal være så begrenset som mulig. Med grunnlag i dette, er det et grunnleggende personvernspørsmål om den kontrollen lagring av alle borgeres elektroniske kommunikasjon innebærer, er nødvendig for å oppnå effektiv kriminalitetsbekjempelse. Denne forholdsmessighetsvurderingen finner vi også igjen i EMK og i EU-retten generelt. Det må altså foretas en grundig vurdering av om lagring av data er *nødvendig* for å bekjempe alvorlig kriminalitet, slik formålet fremkommer i

direktivet. Dersom denne vurderingen konkluderer med at datalagring er nødvendig, er det viktig å legge til rette for så personvernvennlige løsninger som mulig. Spørsmål om lagringstid, lagringssted, sikring og tilgang til data må vurderes nøye, og løsningene må balanseres mot det inngrepet i personvernet som datalagringen representerer.

Samtidig er det viktig å forsøke å sette effekten av lagring av data inn i en større registreringssammenheng. Vi lever i et samfunn som preges av stadig flere kontrolltiltak begrunnet i ønsket om å sikre borgernes trygghet og sikkerhet, og i hensynet til effektivitet. Borgerne registreres og kontrolleres på stadig flere samfunnsområder. Dette er blant annet et resultat av at vi benytter flere elektroniske tjenester, at stadig flere betalinger skjer ved hjelp av elektroniske betalingsmidler og at vi gjør utstrakt bruk av elektronisk kommunikasjon. Samlet finnes det enorme mengder elektroniske spor knyttet til hver og en av oss. Sporene gjør det mulig å gjenskape den enkeltes bevegelser og aktiviteter på et relativt detaljert nivå. Når det vurderes å legge til rette for ny registrering av personopplysninger, nye kontrollmuligheter og ny bruk av elektroniske spor, er det derfor viktig å sette tiltakene inn i en helhet, og vurdere effekten av tiltaket sammen med andre registrerings- og kontrolltiltak som borgerne utsettes for. Konkret betyr dette at effekten av datalagring ikke bare er et spørsmål om personvern på den ene siden, og kriminalitetsbekjempelse på den andre, men også er et spørsmål om å sette effekten av datalagring inn i samfunnets totale kontrollbilde. I forbindelse med innføring av nye og inngripende tiltak, er det nødvendig å se sammenhenger mellom de ulike tiltakene, og totaleffekten av dem. Hver for seg kan tiltakene være akseptable, men samlet kan de utgjøre et uakseptabelt inngrep. Dette aspektet må også være en del av personvernvurderingen når gjennomføring av datalagringsbestemmelser skal avgjøres.

Det tredje hensynet som må vurderes og avveises ved innføring av en lagringsplikt i norsk rett er konkurransen innenfor markedet for elektronisk kommunikasjon. Som nevnt innledningsvis er formålet med datalagringsdirektivet å harmonisere regelverket for datalagring for å sikre at det indre marked fungerer. Intensjonen er at tilbydere av elektroniske kommunikasjonsnett og -tjenester skal stå overfor de samme regulatoriske forpliktelsene innenfor det indre marked. Som det ble nevnt ovenfor overlater direktivet til nasjonale myndigheter å ta stilling til flere sentrale spørsmål som får betydning for tilbydere av elektroniske kommunikasjonsnett og -tjenester, som for eksempel administrative og økonomiske kostnader. Det er viktig at den økonomiske og administrative belastningen ikke fører til konkurransevridning og etableringshindring i markedet for elektronisk kommunikasjon. Det er også viktig at forholdene legges best mulig til rette slik at byrdene på tilbyderne ved gjennomføringen av direktivet ikke blir så store at mindre tilbydere i spredtbygde strøk av landet må innstille virksomheten.

4.2 **Forholdet til Den europeiske menneskerettighetskonvensjonen (EMK)**

Datalagringsdirektivet har en side til Den europeiske menneskerettighetskonvensjon (EMK) artikkel 8 som gjelder retten til respekt for privatliv, familieliv, hjem og korrespondanse som lyder:

”1. Enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin korrespondanse.

2. Det skal ikke skje noe inngrep av offentlig myndighet i utøvelsen av denne rettighet unntatt når dette er i samsvar med loven og er nødvendig i et demokratisk samfunn av hensyn til den nasjonale sikkerhet, offentlige trygghet eller landets økonomiske velferd, for å forebygge uorden eller kriminalitet, for å beskytte helse eller moral, eller for å beskytte andres rettigheter og friheter.”

EMK er gjort til en del av norsk rett ved lov 21. mai 1999 nr. 30, jf § 2. Ved motstrid med annen lovgivning skal bestemmelsene i bl.a. EMK ha forrang, jf. loven § 3.

Når myndighetene pålegger private aktører å lagre data eller krever data utlevert fra private aktører, kan det være et inngrep i retten til privatliv, herunder korrespondanse slik dette må forstås i lys av dagens teknologi. Vi legger til grunn at direktivet medfører inngrep i privatlivet på en slik måte at det omfattes av EMK artikkel 8 nr. 1. Spørsmålet blir så om inngrepet kan rettferdiggjøres etter EMK artikkel 8 nr. 2. Inngrepet må da ha hjemmel i lov og være nødvendig i et demokratisk samfunn for å oppfylle et legitimt formål. Lovkravet er oppfylt gjennom forslaget til ekomloven § 2-8 nytt annet ledd.

Formålet med lagringsplikten er bl.a. å gi politiet et effektivt virkemiddel i bekjempelsen av grov kriminalitet og i sin ytterste konsekvens å vareta den nasjonale sikkerheten. En tilbyder kan derfor bli pålagt å utlevere lagringspliktig data dersom dataene er nødvendig for etterforskningen av alvorlig kriminalitet. I lovforslaget er i tillegg enkelte typer lovbrudd hvor utlevering av data antas å være et særlig effektivt tvangsmiddel i etterforskningen, men som har en lavere strafferamme, foreslått som alternative hjemler for utlevering. Både forebygging av kriminalitet og hensynet til nasjonal sikkerhet er legitime formål etter EMK artikkel 8 nr. 2.

Det springende punktet blir således om inngrepet er nødvendig i et demokratisk samfunn for å oppnå formålet om å bekjempe kriminalitet og vareta den nasjonale sikkerheten. Ved vurderingen av hvilke tiltak det er nødvendig å iverksette for å vareta den nasjonale sikkerheten og bekjempe kriminalitet, må statene ha en stor skjønnsmargin. Hvor inngripende tiltaket er, vil også ha konkret betydning for vurderingen av om inngrepet er nødvendig.

Det inngrepet det her er tale om, er lagring, og eventuelt senere utlevering, under strenge vilkår, av data. Selv om lagringsplikten gjelder alle brukere av elektronisk kommunikasjon, er inngrepet samtidig mindre inngripende for den enkelte enn for eksempel telefonavlytting. Lagringen vil dessuten bare være for en tidsavgrenset periode. Endelig vil dette ikke gjelde informasjon som er direkte knyttet til folks personlige identitet. For eksempel dreier lagringsplikten seg om å lagre at det på et gitt tidspunkt gikk en e-post fra en IP-adresse til en annen. Slike data er således ikke direkte knyttet til en persons identitet på linje med fingeravtrykk eller DNA. For politiet kan det derimot ha stor nytteverdi i bekjempelsen av alvorlig kriminalitet og varetakelsen av

den nasjonale sikkerheten å vite at det kan ha vært kontakt mellom to personer eller miljøer.

Inngrep bør likevel ikke gå lenger enn det som er nødvendig for å oppnå formålet om kriminalitetsbekjempelse og å vareta den nasjonale sikkerheten. Det må derfor vurderes om formålet like effektivt kan oppnås med tiltak som ikke gjør inngrep i privatlivet eller som er mindre inngripende. I dag er det en kjensgjerning at en stadig større del av kommunikasjonen mellom mennesker skjer ved hjelp av elektronisk kommunikasjon. Etterforskningsmetodene må tilpasses denne utviklingen. Samtidig må man være klar over at nettopp det faktum at svært mye kommunikasjon foregår elektronisk, medfører at datalagring åpner for etablering av de registrertes kontaktnett på en måte som ikke tidligere var mulig, og som av mange vil kunne oppleves som inngripende. Lagringstiden vil ha betydning for mengden lagret informasjon, og dermed hvor detaljert dette kontaktnettet kan gjenskapes av politiet. I vurderingen av om omfanget av inngrepet tilfredsstiller nødvendighetskriteriet, vil også lagringstidens lengde være relevant.

I dag varierer det noe fra tilbyder til tilbyder om det lagres data, samt eventuelt hvor mye som lagres. Uten en konsekvent lagringsplikt for alle tilbydere, kan det være noe tilfeldig hva politiet får tilgang til av data. En praksis hvor kriminalitetsbekjempelse og varetakelse av den nasjonale sikkerhet beror på tilfeldigheter må i det lange løp betegnes som utilfredsstillende. Departementene har vurdert problemstillingen, og kan ikke se at det finnes andre alternativ som kan erstatte datas betydning i etterforskningen av alvorlig kriminalitet. Dette kan således tale for at lagringsplikten er nødvendig i et demokratisk samfunn for å bekjempe kriminalitet og vareta den nasjonale sikkerheten.

Etter dette legger departementene til grunn at plikten til å lagre data som nedfelt i datalagringsdirektivet, ikke er i strid med EMK artikkel 8. Det er også den konklusjon EU har kommet til, jf. fortalen punkt (9) som lyder (i dansk versjon):

"(9) Ifølge artikel 8 i konventionen til beskyttelse af menneskerettigheder og grundlæggende frihedsrettigheder (den europæiske menneskerettighedskonvention) har enhver ret til respekt for sit privatliv og familieliv, sit hjem og sin korrespondance. Offentlige myndigheder må kun gøre indgreb i udøvelsen af denne ret, hvis det sker i overensstemmelse med loven og er nødvendigt i et demokratisk samfund af hensyn til bl.a. den nationale sikkerhed og den offentlige tryghed for at forebygge uro eller forbrydelse eller for at beskytte andres rettigheder og friheder. Da lagring af data har vist sig at være et sådant nødvendigt og effektivt efterforskningsredskab for retshåndhævelsen i flere medlemsstater, herunder navnlig i alvorlige sager som organiseret kriminalitet og terrorisme, er det nødvendigt at sikre, at de lagrede data er tilgængelige i forbindelse med håndhævelsen af loven i en vis periode på de vilkår, der er fastsat i dette direktiv. Vedtagelsen af et instrument til lagring af data, der er i overensstemmelse med kravene i artikel 8 i den europæiske menneskerettighedskonvention, er således en nødvendig foranstaltning."

4.3 **Kriminalitetsbekjempelse i en ny teknologisk hverdag**

Samfunnsutviklingen påvirker politiets oppgaver, oppgaveløsning og arbeidsvilkår, som den gjør på de fleste samfunnsområder. Den teknologiske og sosiale utviklingen, og de rettspolitiske rammebetingelsene er avgjørende for politiets oppgaver og oppgaveløsning. En globalisert verden er preget av rask og omfattende flyt av varer, kapital, personer og informasjon. Landegrensene blir stadig mindre viktig i forhold til sosial og økonomisk samhandling. Hendelser ett sted i verden får i økende grad betydning for enkeltmennesker, virksomheter og samfunn andre steder.

Utvikling og utbredelse av ny teknologi endrer stadig rammebetingelsene for samhandling og kommunikasjon mellom mennesker nasjonalt og internasjonalt. Utbredelse av Internett, e-post og mobiltelefoner er eksempler på dette. Teknologiutviklingen går stadig raskere og innvirkningen på samfunnet i takt med den. I kjølvannet av den teknologiske utviklingen har også nye kriminalitetsformer oppstått, slike som datainnbrudd, databedrageri og elektronisk dokumentfalsk. Den nye kriminaliteten muliggjøres av den nye teknologien.

Disse utviklingstrekkene representerer flere utfordringer for politiet, men også muligheter i kriminalitetsbekjempelsen. Teknologiutviklingen har gitt de kriminelle nye muligheter til å utføre kriminelle handlinger og til å unndra seg kontroll og straffeforfølging, men når lovbrudd dokumenteres og distribueres elektronisk, etterlates det også elektroniske spor. Slik sett representerer IKT-utviklingen også en mulighet for å forebygge, avdekke og etterforske lovbrudd effektivt.

4.4 **Hva skal lagres**

Det fremgår av datalagringsdirektivets artikkel 5 hvilke kategorier av data som skal lagres. Forslaget til lovendring som presenteres i dette høringsnotatet vil medføre innføring av lagringsplikt for trafikkdata, lokaliseringsdata og abonnements/brukerdata som fremkommer ved bruk av elektronisk kommunikasjon som fasttelefon, mobiltelefoni, internettaksess, e-post og bredbåndstelefoni. EUs datalagringsdirektiv lister opp kategorier av data som skal lagres, og i det følgende skisseres departementenes vurdering av de nevnte kategoriene.

Samlet vil lovendringen representere en utvidelse av hvilke opplysninger som skal lagres sett i forhold til hva som faktisk lagres i dag. Dette skyldes først og fremst at det skal lagres opplysninger som vil kunne være tilgjengelig i dag, men som bare i begrenset grad blir lagret, så som bruk av e-post og internettilgang. Dertil kommer at kretsen av de som skal lagre opplysninger utvides når lagringspliktige opplysningstyper utvides, f eks ved at tilbydere av internettilgang underlegges lagringsplikt langt ut over den faktiske langringen disse foretar i dag. Det er likevel viktig å presisere at alle tilbydere ikke skal lagre alt. Hver tilbyder skal kun lagre de data som fremkommer når de ufører sin tjeneste, det vil si bare data de har tilgang til, jf. direktivets fortale punkt 13. Det fremgår av samme fortale at innhold ikke skal lagres, og at data skal lagres på en slik måte at man unngår at de blir lagret mer enn én gang. Departementene ser at

det i praksis kan være vanskelig å unngå dobbeltlagring, all den tid verdikjeden for produksjon av ekomtjenester er kompleks og man vil oppleve at enkelte data vil være tilgjengelig hos flere tilbydere samtidig. De ulike tilbyderne har dessuten per i dag skreddersydde løsninger for kommunikasjons- og faktureringsformål som de fortsatt vil kunne måtte benytte.

Som presisert ovenfor fremsetter direktivet krav om at hver tilbyder kun skal lagre de data som fremkommer når de ufører sin tjeneste, det vil si de data som de har tilgang til, og som inngår i opplistingen nedenfor.

EU-direktivets opplisting kan gi rom for tolkning. Det er departementenes oppfatning at punktene nedenfor er en nødvendig presisering av hva som skal lagres i henhold til direktivet. Departementene ber om høringsinstansenes syn på presiseringen av hva som eventuelt skal lagres.

Dersom datalagringsdirektivet skal innføres i norsk rett foreslår departementene at det stilles krav om lagring på de områdene som fremgår i kapittel 4.4.1 – 4.4.5 nedenfor:

4.4.1 Ved fasttelefoni skal følgende data lagres

- A-nummer: oppringers telefonnummer
- B-nummer: telefonnummer til den som blir oppringt
- C-nummer: telefonnummer til videresendt abonnement
- abonnent/brukerdata og registrert bruker/identitet for eier av A, B og C nummer
- dato og tidspunkt ved start og avslutning av kommunikasjon

4.4.2 Ved mobiltelefoni skal følgende data lagres

- A-nummer: oppringers telefonnummer
- B-nummer: telefonnummer til den som blir oppringt
- C-nummer: telefonnummer til videresendt abonnement
- de internasjonale IMEI/IMSI identiteter for A- B- og C- nummer
- abonnent/brukerdata og registrert bruker/identitet for eier av A, B og C nummer
- dato og tidspunkt ved start og avslutning av kommunikasjon
- informasjon om hvilken kommunikasjonstjeneste som er benyttet
- lokaliseringsinformasjon ved start og avslutning av kommunikasjon

I de fleste tilfeller gir det seg selv hvem som skal lagre hva. For en tilbyder av fasttelefoni og mobiltelefoni vil ansvaret for lagring stoppe ved et eventuelt samtrafikkpunkt. Tilbyderen må kunne gi informasjon om hvem samtrafikkpartneren er.

4.4.3 Ved bredbåndstelefoni skal følgende data lagres

- IP-adresser som identifiserer oppringer og den som blir oppringt
- tildelt brukeridentitet
- navn og adresse til abonnent eller registrert bruker som IP-adresse eller/og telefonnummer ved oppringt tjeneste
- brukeridentitet eller telefonnummer som tildeles den eller de som er mottaker av en bredbåndstelefonisamtale
- informasjon som identifiserer kommunikasjonsutstyr eller kommunikasjonsanlegg

4.4.4 Ved internettaksess skal følgende data lagres

- brukers IP-adresse
- abonnentinformasjon, registrert brukerinformasjon
- dato og tidspunkt for pålogging og avlogging av internettjenesten
- type internettoppkobling
- informasjon som identifiserer kommunikasjonsutstyr eller kommunikasjonsanlegg

Informasjon om bruk av Internett lagres i dag i en svært begrenset periode for driftsrelaterte formål, og maks tre uker, jf Datatilsynets vedtak fra mai 2009. Lagring av denne type opplysninger i medhold av direktivet, vil således være en betydelig utvidelse i forhold til gjeldende regime.

4.4.5 Ved e-post skal følgende data lagres

- avsender og mottakers e-postadresse og IP-adresser
- abonnentinformasjon og registrert brukerinformasjon
- dato og tidspunkt for pålogging og avlogging til e-posttjenesten

4.4.6 Mislykkede oppringninger

Det fremgår av datalagringsdirektivet at relevante data som genereres i forbindelse med mislykkede oppringinger og mislykkede påkoblinger skal omfattes av lagringsplikten i lovforslaget. Mislykkede oppringinger/påkoblinger er oppkoblinger hvor tilbyderne har gjort oppringningen tilgjengelig for oppringte, men oppringte besvarer ikke anropet. Det stilles derimot ikke krav i datalagringsdirektivet om at data knyttet til oppringinger/påkoblinger som ikke oppnår forbindelse skal lagres. Dette er oppringninger hvor tilbyder ikke klarer å koble opp forbindelse frem til B-nummeret.

4.4.7 Nærmere om innhold

Innholdet, eller noe som avslører innholdet i kommunikasjonen, omfattes ikke av tilbyders lagringsplikt. Med "avslører innholdet" mener departementene at det ikke skal lagres data som viser eller tilkjennegir kommunikasjonens innhold. For eksempel

om en bruker surfet på en gitt webside, innholdet i en SMS/MMS eller innholdet i en e-post. Tilgang til en brukers IP-adresse gir i dag ikke automatisk en oversikt over hvor det har vært surfet, altså innholdet på web-sidene som har blitt besøkt. Skal politiet finne ut av dette må de ha tilgang til brukers datamaskin eller det må gjøres mer etterforskningsarbeid med tanke på å kontrollere hvem som eide en gitt IP-adresse på et angitt klokkeslett osv.

Ved benyttelse av applikasjoner som ikke er definert som offentlige ekomtjenester, det vil si tjenester som tilbys av andre enn tilbydere definert i ekomloven, vil data i tilknytning til kommunikasjonen ikke bli lagret. Eksempel på slike tjenester er Skype, som i utgangspunktet er en taletjeneste, men som det også er mulig å sende multimediameldinger og tekstmeldinger fra. MSN er en chattetjeneste som også omfatter tale, video, oversendelse av dokumenter/filer. Ved benyttelse av disse tjenestene vil ISPen som kobler tjenesten lagre data om at brukeren er på nettet, men ISPen har ingen mulighet til å identifisere hvilke tjenester som benyttes og hvem som kommuniserer med hvem. For at politiet skal ha mulighet til å hente ut data og innhold når slike applikasjoner benyttes, må det gjennomføres "sanntids" kommunikasjonskontroll.

I henhold til datalagringsdirektivets artikkel 3 er det kun data som rent faktisk fremkommer hos tilbydere av elektroniske kommunikasjonsnett og -tjenester som skal lagres i henhold til lovforslaget. Det avgjørende for lagringsplikten er hvorvidt utførsel av en ekomtjeneste de facto prosesserer eller behandler relevante data. Dette innebærer med andre ord at lagringsplikten bare er aktuell der det i forbindelse med fasttelefontjeneste, mobiltelefontjeneste, internettaksess, bredbåndstelefonitjeneste og e-posttjeneste fremkommer relevante data i det elektroniske kommunikasjonsnettet. I denne sammenheng menes med relevante data trafikkdata, celle-ID og data nødvendig for å identifisere abonnent eller bruker.

4.5 **Lagring av andre data**

I forslaget til lovbestemmelse § 2-8 første ledd i ekomloven foreslås eventuelt innført en plikt til å lagre data. Bestemmelsen skisserer hvilke data som skal lagres. Ved produksjon av elektronisk kommunikasjonstjeneste produseres og genereres det også andre data utover de som er nevnt i oppramsingen i kapittel 4.4. Dette vil kunne være data som benyttes til faktureringsformål og andre kommunikasjonsformål. Disse dataene skal i henhold til forslaget slettes så snart de ikke lenger er nødvendige for kommunikasjons- eller faktureringsformål. Dette vil være en videreføring av dagens praksis.

4.6 **Hvem skal lagre i henhold til lovforslaget**

I henhold til datalagringsdirektivet er det tilbydere av offentlig elektronisk kommunikasjonsnett eller -tjeneste som skal lagre dataene. Lagringsplikten gjelder mobilnett og mobiltelefontjeneste, fastnett og fasttelefontjeneste, internettaksess,

bredbåndstelefoni og e-post. Departementene legger til grunn at begrepene tilbyder, offentlig elektronisk kommunikasjonstjeneste og elektronisk kommunikasjonsnett som anvendes til offentlig elektronisk kommunikasjonstjeneste har samme innhold som etter gjeldende ekomlov. Det vil si at enhver fysisk eller juridisk person som tilbyr andre tilgang til elektronisk kommunikasjonsnett som anvendes til offentlig elektronisk kommunikasjonstjeneste eller tilbyder av slik tjeneste, har lagringsplikt med de begrensninger som følger av kapittel 4.4 over. Som det fremgår av kapittel 2.5 forholder politiet seg i praksis i til Telenor og NetCom når det gjelder uthenting av trafikkdata, fordi det i hovedsak har vært trafikkdata knyttet til fasttelefonitjeneste og mobiltelefonitjeneste som har blitt etterspurt. Ved en eventuell innføring av en lagringsplikt vil alle tilbydere måtte lagre, også tilbydere av bredbånd og bredbåndstjenester.

Elektronisk kommunikasjonstjeneste er i ekomloven § 1-5 definert som "tjeneste som helt eller i det vesentlige omfatter formidling av elektronisk kommunikasjon og som normalt ytes mot vederlag". Når det gjelder offentlighetsbegrepet er det etter ekomlovens definisjon avgjørende om tjenesten er tilgjengelig for allmennheten eller beregnet til bruk for allmennheten, jvf. § 1-5, nr 7. Ved vurderingen av om tjenesten tilbys allmennheten, skal det blant annet legges vekt på antall brukere og interessefellesskapet mellom disse. Det legges til grunn at for eksempel borettslag med private nett normalt ikke vil være omfattet av dette tilbyderbegrepet. Andre eksempler på virksomheter som normalt faller utenfor dette tilbyderbegrepet er bedrifter, sykehus, hoteller og lignende som utelukkende stiller elektroniske kommunikasjonstjenester til rådighet for sine kunder eller ansatte. Det vil være myndigheten etter ekomloven som i de enkelte grensetilfelle avgjør om det er snakk om en offentlig tjeneste.

Departementene er kjent med at det knytter seg usikkerhet til hvorvidt tilbydere av web-basert e-post og andre web-baserte applikasjoner vil omfattes av datalagringsdirektivet. Det må her for hver tjeneste vurderes om det tilbys tilgang til offentlig elektronisk nett- eller kommunikasjonstjeneste. Departementene viser her til veilederen fra EU-kommisjonens ekspertgruppe om dette, datert 27. juli 2009, der det fremgår at "the provider must be considered individually to determine if it is a provider that falls within the legal limitation of scope enshrined in the Directive".

Det følger som nevnt av datalagringsdirektivet at man bør søke å unngå at de relevante trafikkdata lagres mer enn en gang. Når det gjelder forhold hvor en tilbyder leverer elektroniske kommunikasjonstjenester til bedrifter og lignende, vil det praktiske utgangspunktet derfor være at dataene bare skal lagres hos den tilbyderen som leverer tjenesten.

Gjeldende hjemmel for myndigheten til å gi forskrift om tilretteleggingsplikt, herunder plikt til å lagre trafikkdata, tenkes videreført slik at det kan pålegges andre enn de som faller inn under tilbyderbegrepet en lagringsplikt dersom dette er nødvendig for å oppnå formålet med bestemmelsen. Dette foreslås også å kunne gjøres ved enkeltvedtak i fremtiden. Det kan være tilfeller der det ikke er hensiktsmessig eller

nødvendig for å oppnå formålet med bestemmelsen å pålegge enkelte tilbydere som faller innenfor definisjonen å skulle lagre. I slike tilfeller foreslås det å kunne gjøre unntak ved enkeltvedtak.

4.7 **Ulike løsninger for lagringssted**

EUs direktiv presiserer som nevnt at man bør unngå å lagre data mer enn én gang, men utover dette legger direktivet ikke noen føringer på hvordan lagringen skal foregå, med unntak av minimumsbestemmelser om datasikkerhet.

Som nevnt ovenfor fikk departementene i 2006 utredet kostnadene knyttet til ulike lagringsmodeller. Utredningen var avgrenset til kostnader knyttet til lagring av data fremkommet ved bruk av fasttelefoni, mobiltelefoni og internettaksess. To hovedmodeller har blitt utredet: lagring hos tilbyder og lagring i en sentral database. Departementene har også sett på ulike mellomløsninger som for eksempel valgfri lagring i sentral base og kjøp av lagringskapasitet hos selskaper med dette som sitt spesialfelt. Det er viktig å understreke at betingelsene og vilkårene for å få tilgang til dataene vil være de samme uavhengig av hvor lagringen eventuelt skulle skje. I det følgende beskrives kort de ulike modellene som Teleplan utredet i 2006.

4.7.1 Lagring hos tilbyder

I modellen skissert av Teleplan lagres data hos tilbyderne, og data hentes ut av tilbyderne. Det er i modellen forutsatt at det settes opp egne lagringsløsninger for data som lagres til myndighetenes formål atskilt fra forretningsmessige data. For de små tilbyderne har Teleplan antatt at de vil klare seg med relativt enkle verktøy for å hente ut data. For de større tilbyderne har Teleplan antatt at det vil være mer omfattende å sette opp lagringsløsninger med mekaniser for å søke etter og hente ut data.

4.7.2 Lagring i sentral database

Departementene har fått utredet en lagringsløsning hvor tilbyderne overfører data til en sentral database. Samferdselsdepartementet og Justis- og politidepartementet ønsket lagringsmodellen utredet med bakgrunn i en antakelse om at en slik løsning vil kunne ha mange fordeler knyttet til forenkling av den praktiske prosessen for politiet, samt fordeler når det gjelder sikkerhet og kontroll. Modellen forutsetter at alle tilbyderne plikter å overføre data til den sentrale databasen. Tilbyderne må selv hente ut og konvertere dataene fra sitt lagringsformat til et standardisert format før de oversendes til en slik sentral base. For at løsningen skal være praktisk å bruke forutsetter Teleplan at data blir overført fra tilbyderne til den sentrale basen en gang i døgnet. Inkludert i løsningen Teleplan skisserer er en portal for myndighetene og søkemekanismer.

4.7.3 Mellomløsninger

En mellomløsning kan være at myndighetene etablerer en sentral database som det er frivillig for tilbyderne å knytte seg til. For små tilbyderne vil dette være å foretrekke forutsatt at staten dekker driftsutgiftene for databasen. For de større tilbyderne vil dette alternativet fremstå som mindre aktuelt i og med at de allerede har systemer som det antas at de vil bygge videre på. En annen mellomløsning er å legge opp til at bransjen selv etablerer en sentral database. En slik base vil kunne være særlig aktuell for de små tilbyderne for å redusere kostnadene knyttet til lagring. Små tilbydere innenfor et geografisk område vil kunne finne det hensiktsmessig å samarbeide om funksjoner der den enkelte ikke finner det økonomisk forsvarlig å ha egen kompetanse eller kapasitet. Datalagring antas å kunne være et slikt område. Det er videre sannsynlig at det på kommersielt grunnlag vil oppstå løsninger hvor mindre tilbydere tilbys felles lagring. Under arbeidet med høringsnotatet har departementene fått innspill fra enkelte aktører i bransjen som mener at en frivillig basert sentralisert løsning for små tilbydere vil kunne være hensiktsmessig forutsatt at en tredjepart (ikke politiet og ikke en tilbyder) står for lagringen.

4.7.4 Avveining av ulike hensyn ved valg av lagringsløsning

Departementene foreslår at det skal være opp til den enkelte tilbyder å velge lagringsløsning. Flere hensyn er vurdert når det ikke foreslås å etablere en sentral lagringsløsning, selv om det fremstår som den billigste løsningen i Teleplans første analyse. Særlig er personvernmessige hensyn vektlagt. Datatilsynet har gitt uttrykk for bekymring for en sentral lagringsmodell og departementene har valgt å følge Datatilsynets anbefaling på dette området, uten at dette utelukker at små tilbydere kan gå sammen om en lagringsløsning. I tillegg til de personvernmessige vurderingene, har departementene også vurdert kostnader, andre sikkerhetsmessige og konkurransemessige aspekter

4.7.4.1 Lagringsstedets betydning for personvern

Et grunnleggende spørsmål er om det er ønskelig å samle alle trafikkdata på ett sted. En slik samling av store mengder personlig informasjon kan i seg selv sies utgjør en ekstra personvernrisiko. Det ville være en forutsetning for opprettelse av en sentral database at man kan sikre at dataene ikke blir brukt til andre formål enn det som er formålet med opprettelsen. Dette er imidlertid vanskelig å garantere, fordi det alltid vil foreligge en viss fare for utilsiktet utlevering eller misbruk. Og jo mer informasjon som er samlet på ett sted, jo større er skadepotensialet ved eventuelt misbruk av dataene. Datatilsynet har i tillegg vist til at det kan oppstå gråsoner med hensyn til hvem som har behandlingsansvaret for dataene dersom de overføres fra tilbyder til en sentral database. Departementene mener hensynet til trusselen om misbruk og usikkerhet om behandlingsansvar er tungtveiende argumenter mot å foreslå en sentral lagringsløsning. Departementene vil heller la det være opp til den enkelte tilbyder å velge lagringsløsning lokalt.

I henhold til EUs datalagringsdirektiv er det ikke et krav at dataene skal lagres atskilt, men det skal etableres hensiktsmessige tekniske og organisatoriske anordninger for å ivareta datasikkerheten. Artikkel 29- gruppen har pekt på nødvendigheten av å etablere skiller mellom dataene sånn at tilbyderne ikke kan benytte data lagret i henhold til datalagringsdirektivet til eget bruk. Både Datatilsynet og tilbydere av elektroniske kommunikasjonsnett og -tjenester har signalisert at de er enige i Artikkel 29-gruppens anbefaling om at det ved eventuell innføring av en lagringsplikt bør etableres et logisk skille mellom dataene avhengig av dataenes formål. Etablering av et logisk skille mellom data til faktureringsformål og andre administrative formål på den ene siden, og data til kriminalitetsbekjempende formål på den andre siden, er i følge ekomtilbyderne, både teknisk og administrativt uproblematisk, men vil kreve at tilbyderne investerer i lagringsløsninger til formålet.

Signalene fra Artikkel 29 gruppen og tilbydere av ekom bør tas hensyn til. Departementene foreslår derfor at dersom direktivet innføres bør data lagret i henhold til datalagringsdirektivet lagres logisk adskilt fra data tilbyder eventuelt vil måtte lagre til fakturerings- og kommunikasjonsformål. Tilbyder plikter i henhold til lovforslaget å lagre de definerte dataene som lagres i henhold til datalagringsdirektivet, og det er kun politiet som under visse vilkår skal få tilgang til disse dataene.

De generelle kravene til informasjonssikkerhet i personopplysningsloven § 13 med tilhørende forskrifter gjelder fullt ut. Disse reglene, sammenholdt med de faktiske forhold hos den enkelte tilbyder, medfører krav om adskilt lagring. Se for øvrig kapittel 4.7.4.2 om informasjonssikkerhet. Departementene forutsetter at tilbyderne i forbindelse med lagringen oppfyller forpliktelsene i personopplysningslovgivningen når det gjelder behandlingen av dataene. En plikt til å lagre data utover det som i dag gjøres av hensyn til egen forretningsvirksomhet, innebærer ikke at tilbyder får en utvidet adgang til å bruke dataene til egne formål.

4.7.4.2 Lagringsstedets betydning for informasjonssikkerhet

Den største utfordringen med en løsning hvor tilbyderne selv velger lagringsløsning, er at også ansvaret for god datasikkerhet og vern av personopplysninger om den enkelte bruker av elektronisk kommunikasjon ligger hos den enkelte tilbyder. jf personopplysningsloven § 13 og personopplysningsforskriften kapittel 2. Tilbyderne har imidlertid vært underlagt og forholdt seg til dette regelverket i mange år, og bør således være vant til å sikre sine systemer og lagre data i samsvar med personopplysningslovens krav.

Tilbydere av elektroniske kommunikasjonsnett og -tjenester vil, dersom plikt til datalagring skal innføres, i henhold til forslaget stå fritt til å velge lagringsløsning. Som nevnt ovenfor forutsettes det imidlertid at data lagret i medhold av datalagringsplikten, skal holdes logisk adskilt fra andre personopplysninger som lagres og behandles hos ekomtilbyderne. Datalagringsdirektivet skisserer noen konkrete krav til sikkerhet, herunder et prinsipp om at de lagrede dataene skal være av samme kvalitet og nyte

godt av samme beskyttelse og sikkerhetsforanstaltninger som øvrige data generert i det elektroniske kommunikasjonsnettet. I samsvar med personopplysningsloven § 13, skal den behandlingsansvarlige også sørge for passende tekniske og organisatoriske tiltak for å beskytte dataenes tilgjengelighet, konfidensialitet og integritet, dvs. sikre dem mot uønsket ødeleggelse, bortfall eller endring, eller uautorisert eller ulovlig lagring, behandling, tilgjengeliggjøring eller utlevering. Videre er det kun autorisert personell som skal ha tilgang til dataene. Dataene skal, med unntak av opplysninger som har blitt tilgjengeliggjort i samsvar med utleveringsbestemmelser i nasjonal rett eller er oppbevart for videre behandling i samsvar med nasjonal lovgivning, slettes på betryggende måte når lagringsperioden er over.

Ulike mekanismer for informasjonssikkerhet kan i dag integreres i IKT-løsninger. Blant annet kan det innarbeides gode løsninger for logging av tilgang til og bruk av de lagrede dataene. Det er derfor departementenes oppfatning at dersom man skulle innføre en lagringsplikt vil informasjonssikkerheten kunne bli tilstrekkelig ivaretatt ved en desentralisert lagringsløsning, også hos de tilbyderne som per i dag ikke har noe system for lagring.

4.7.4.3 Lagringsstedets betydning for uthenting av data

EUs direktiv legger ingen føringer for hvordan de lagrede data skal hentes ut eller overføres til myndigheten, men det fremgår i artikkel 8 at data skal lagres slik at de på anmodning fra kompetent myndighet kan overføres uten unødvendig forsinkelse. En enkel og praktisk prosess både for politiet og for tilbydere når det gjelder uthenting og utveksling av data er et mål. Samling av data på et sted vil kunne gjøre den praktiske prosessen med å få tilgang til data enklere for politiet i og med at de ved uthenting av data kan forholde seg til én virksomhet i stedet for et stort antall tilbydere. Ved en eventuell rettssak hvor det skulle vise seg å være tvil om datas riktighet ville politiet fortsatt være avhengig av tilbyderne for å få dataene verifisert. Når departementene nå foreslår at det er den enkelte tilbyder som er ansvarlig for å lagre data dersom det innføres en lagringsplikt, blir det viktig å finne løsninger som forenkler den praktiske prosessen både for politiet og tilbyderne. Erfaringene fra dagens ordning med kommunikasjonskontroll og uthenting av trafikkdata er blant annet at politiet har store utfordringer knyttet til uthenting og da særlig hos de mindre tilbyderne. Tilbyderne har i liten grad systemer som er tilpasset myndighetenes behov for trafikkdata. Dataene blir i dag lagret for å dekke forretningsmessige behov og tilbyderne har etablert sine systemer ut fra dette formålet.

4.7.4.4 Lagringsstedets betydning for kostnader

Teleplans økonomiske konsekvensanalyse fra 2006 indikerer at en løsning hvor tilbyderne plikter å overføre dataene til en sentral database totalt sett kan fremstå som noe billigere enn en løsning hvor data lagres hos tilbyder. En mellomløsning hvor myndighetene etablerer en sentral database som kun enkelte tilbydere overfører data til, gir de høyeste kostnadene. Det gir imidlertid ikke nødvendigvis et korrekt bilde å sammenligne løsningene direkte. Dersom man sammenligner tallene for en sentral og

en lokal lagringsløsning må man ta hensyn til at løsningene sannsynligvis implementeres forskjellig og at utviklingstiden for etablering av lagringsløsningen vil være forskjellig for de ulike løsningene. Det må understrekes at kostnadsestimatene som fremgår i Teleplans rapport er svært grove og forutsetter at det er snakk om lik utviklingstid for de ulike løsningene, noe som er lite sannsynlig.

4.7.4.5 Lagringsstedets betydning for konkurransen i ekommarkedet

Formålet med ekomloven er å sikre brukere i hele landet gode, rimelige og fremtidsrettede elektroniske kommunikasjonstjenester, gjennom effektiv bruk av samfunnets ressurser ved å legge til rette for bærekraftig konkurranse, samt stimulere til næringsutvikling og innovasjon, jf ekomloven § 1-1. For ekommyndigheten er det derfor viktig at plikten til å lagre data ikke fører til vridning i konkurransen innenfor markedet for elektronisk kommunikasjon. Formålet med datalagringsdirektivet er å harmonisere regelverket for datalagring sånn at tilbydere av ekomnett og tjenester kan operere under like vilkår innad i et land og med tilnærmet like vilkår i de ulike medlemslandene i EU. Det vil ved en innføring av datalagringsdirektivet fortsatt være variasjoner mellom landene både når det gjelder lagringstid og kostnadsdekning, men i mindre grad enn om man ikke harmoniserer reglene.

På det norske markedet vil en innføring av datalagringsdirektivet medføre at det innføres en plikt til å lagre data, noe som har en kostnad. De største tilbyderne har allerede etablert enkelte systemer for lagring, det gjelder særlig tilbydere av fasttelefonitjeneste og mobiltelefonitjeneste. For disse tilbyderne vil en eventuell innføring av en lagringsplikt medføre at de må lagre mer data og andre typer data enn de gjør i dag for fakturerings- og kommunikasjonsformål. Dette har en kostnad, jf. kapittel 6, men det er departementenes vurdering at det ikke blir for denne kategorien tilbydere at belastningen med å innføre direktivet vil bli tyngst. Det som blir viktig for myndighetene er å sørge for at plikten til å lagre data ikke blir så kostnadsdrivende at det blir en etableringshindring for små tilbydere. Det er også viktig å unngå en utvikling der mindre tilbydere må legge ned sin virksomhet på grunn av for store investeringskostnader. Dette vil i så fall kunne gå sterkt utover tilbudet av tjenester i hele landet.

Departementenes forslag om at tilbyderne selv kan velge lagringsløsning, gir rom for den enkelte tilbyder til å finne mest mulig hensiktsmessige, økonomisk effektive og sikre lagringsløsninger.

I drøftingen ovenfor er det lagt til grunn at tilbydere på det norske markedet eventuelt vil lagre data i Norge eller i de landene som tilbyderne har sitt hovedknutepunkt for svitsjing av trafikk. Ethvert pålegg overfor tilbyderne om å skulle lagre på norsk territorium vil etter forholdene kunne ses på som en begrensning til prinsippet om fri flyt av data innenfor EØS. Det er tenkelig at tilbydere som tilbyr tjenester i flere medlemsland av kommersielle årsaker ønsker å sentralisere sin lagring av data på ett sted. Dette er en utfordring i forhold til datalagringsdirektivet, særlig med tanke på at

det vil kunne være ulike regler som gjelder i ulike land både når det gjelder lagringstid, informasjonssikkerhet og vilkår for uthenting av data.

EU-kommisjonens ekspertgruppe har laget et utkast til veileder om nettopp denne problemstillingen, og det fremgår av utkastet at prinsippet om fri flyt av data innenfor EU gir tilbyderne anledning til å lagre data i et annet land enn det de er etablert i. Dersom det er ulik lagringstid mellom det landet som tilbyderen er etablert i og det landet som tilbyderen ønsker å lagre sine data i, er det førstnevnte lands regler som gjelder. Tilbydere som ønsker å lagre data i en sentral database i EU må sørge for at data fra de ulike medlemslandene er fysisk adskilte, sånn at hvert enkelt medlemslands lover og regler når det gjelder lagringstid, vilkår for uthenting m.m. kan ivaretas.

4.8 **Lagringstid**

EU-direktivet fastslår i artikkel 6 at de relevante data skal lagres for en periode mellom seks måneder og to år. Lagringsperioden bør etter departementenes oppfatning balansere hensynet til kriminalitetsbekjempelse og hensynet til personvern. Hensynet til personvern tilsier at de relevante data ikke skal lagres lengre enn nødvendig av hensyn til kriminalitetsbekjempelse.

Det foreligger ingen statistikk over hvor gamle data politiet har etterspurt til nå. Dagens regelverk inneholder en sletteplikt, utover faktureringsformål og kommunikasjonsformål, som fører til at tilbyderne sletter data etter tre og fem måneder, jf kapittel 2.2. Politiet ber normalt ikke om data som er eldre enn tre og fem måneder fordi tilbyder ikke har anledning til å lagre slike data. En statistikk over politiets forespørsler ville neppe kunnet gi noen indikasjoner på politiets behov for lagring utover fem måneder.

Telenor har på forespørsel fra Datatilsynet informert om at heller ikke Telenor har tallført data for henvendelser til selskapets eget politisvarsenter. Telenor oppgir imidlertid at politisvarsenterets generelle inntrykk er at etterspørselen etter trafikkdata fra politiets side i stor grad gjelder tidsperioder som ligger innenfor de siste tre måneder, eller gjelder trafikkdata for en hel tremåneders periode. Telenor fremhever imidlertid at spørsmål etter gamle data ikke fremmes av politiet fordi politiet vet at Telenor ikke har dem. Samferdselsdepartementet har forespurt alle referansegruppens representanter om tall og inntrykk vedrørende hvilken tidsperiode politiets forespørsler relaterer seg til, og synspunktene er sammenfallende med Telenors.

Det er ved etterforskningen av de alvorligste straffesakene at behovet for lagringstid ut over seks måneder er spesielt stort. Sedelighetssaker, især saker som gjelder seksuell utnyttelse og andre overgrep mot barn, samt alvorlige vinnings-, volds- og narkotikalovbrudd, blant annet innenfor organiserte kriminelle miljøer, er komplekse, og internasjonale relasjoner gjør etterforskningen ytterligere omfattende og tidkrevende. I tillegg kommer saker relatert til avverging av mulig terrorvirksomhet. Politiet erfarer i dag at de ikke får tilgang på nødvendige data fordi disse rettmessig er slettet av tilbyderne. ENEA-saken (seksuelle overgrep mot barn på internett), Finance

Credit-saken og NOKAS-ranet er eksempler på saker som har tatt flere år å etterforske og hvor politiet har erfart at elektroniske spor forsvinner mens etterforskningen pågår, på grunn av ekomtilbydernes sletteplikt.

Politiet erfarer at også 12 måneders lagring vil kunne være for lite. Spesielt i saker om organisert kriminalitet strekker etterforskningen seg som regel over lang tid, og ofte vil perioden fra oppstart av etterforskningen til det tas ut tiltale være over 12 måneder. Dersom det dukker opp nye forklaringer og momenter under førstegangsbehandlingen, kan dette også utløse nytt behov for å innhente data helt tilbake fra oppstart av etterforskningen. Disse bevisene, som kunne opplyst saken, er da normalt slettet og dermed tapt. Et annet hensyn som taler for en lengre lagringstid er at det er en tidkrevende prosess for politiet å kartlegge alle nummer som de impliserte kan ha benyttet.

For domstolene kan bevisvurderingene være problematiske, særlig gjelder dette i mange sedelighetssaker. Det strenge beviskravet medfører at ofre kommer til kort når deres forklaring står alene som bevismoment mot tiltalte. Lagrede data og påfølgende elektroniske spor kan i flere saker være de avgjørende bevisstøttepunkter som domstolen behøver, sammen med de øvrige bevis for å være tilstrekkelig sikker, slik at et hendelsesforløp kan legges til grunn som bevist ut over enhver rimelig og fornuftig tvil. Det er liten tvil om at data som viser elektronisk kontakt mellom mistenkte og fornærmede på angitte tidspunkter, har betydning i slike saker. Manglende trafikkdata på grunn av for kort lagringstid innebærer en selvforsterkende svekkelse av bevissituasjonen. Menneskelig glemsel fører naturlig nok til at forklaringer som bevis svekkes når det har gått noe tid av betydning. Samtidig med tidsforløpet slettes trafikkdataene som følge av kort lagringstid. Den manglende adgangen til å "oppfriske" hukommelsen til et vitne med tidspunkter m.v. fra data, eller å undersøke riktigheten av en allerede avgitt forklaring med opplysninger fra data, innebærer at det blir vanskeligere å oppnå tilstrekkelig opplysning av saken.

Selv om det er påtalemyndighetens ansvar å belyse saken, kan korte slettefrister for data fremkommet ved bruk av elektronisk kommunikasjon også medføre flere situasjoner der siktedes forsvar kommer i underbalanse. For det første i saker hvor det er tatt ut siktelse uten at politiet har funnet det nødvendig å innhente data. For det annet kan kort slettefrist stenge for siktedes mulighet til å innhente ytterligere data, foranlediget av at politiet har fremlagt data som fra siktedes ståsted ikke opplyser saken tilstrekkelig og for det tredje kan forklaringer avgitt under domstolens behandling av straffesaken foranledige fremleggelse av (nye) data, evt. i ankeinstansen. Det kan således oppstå situasjoner hvor siktede ikke får tilstrekkelig tid eller mulighet til å forberede forsvaret. En slik underbalanse kan komme i konflikt med siktedes minsterettigheter etter EMK art. 6 nr. 1 jfr. nr. 3 bokstav b) (herunder prinsippet 'equality of arms'). I saker hvor man opplever at siktede ikke har hatt den samme bevisadgang som påtalemyndigheten, er det betimelig av forsvaret å påpeke en urettferdig prosess og faren for en domfellelse basert på uriktig eller utilstrekkelig grunnlag. Imidlertid vil siktedes manglende tilgang til trafikkdata ofte sette domstolen i

en så vanskelig situasjon at den ser seg nødt til å avsi frifinnende dom i en sak som for øvrig fremstår som godt fundert. Dette viser kompleksiteten.

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. At politiet var i stand til å knytte de NOKAS-dømte til hverandre, skyldtes imidlertid at en av tilbyderne hadde en lengre lagringspraksis enn den andre (Telenor/NetCom). Det fremstår som lite ønskelig at avsløringen av store straffesaker skal bero på tilfeldige avvik i lagringsperioden mellom tilbyderne. Det har også blitt fremhevet at organiserte kriminelle vil tilpasse seg den kontroll som datalagringsplikt innebærer, og at de vil kamuflere sporene sine. Også her brukes NOKAS-saken som eksempel, hvor de involverte var svært bevisst i bruken av mobiltelefoner i forkant av ranet. Automatisk lagring innebærer en betydelig ulempe for organisert kriminelle. Enhver er i dag avhengig av, og tar for gitt, elektronisk kommunikasjon i mange ulike former. Når organisert kriminelle bevisst må forholde seg til slik kontroll, blir det vanskeligere å begå alvorlig kriminalitet. Datalagring har dermed en klart kriminalitetsdempende sidevirkning, dvs. kriminalitetsforebyggende. De organisert kriminelles vilje til å tilpasse seg en lagringsperiode, taler for at det fastsettes en lengre lagringstid. Ved planlegging av et større bankran vil det være praktisk mulig for organisert kriminelle å forholde seg til en 6-månedersfrist ved bruk av elektronisk kommunikasjon, noe NOKAS-saken indikerte. Imidlertid vil det være praktisk svært vanskelig å avholde seg fra slik kommunikasjon i et helt år, uten å kunne knyttes til de personer som man har involvert i planleggingen av for eksempel et stort ran. Denne omstendigheten taler for lengre lagringstid.

Begrunnelsen for ikke å innføre lengre lagringstid enn seks måneder, som er direktivets minimums lagringstid, er i hovedsak personvernmessige hensyn. I dag lagres trafikkdata i maksimalt fem måneder. Seks måneders lagringstid vil således være en utvidelse av lagringstiden i forhold til gjeldende rett. Politiet vil dermed få potensiell tilgang til informasjon for en lengre tidsperiode enn de i dag har. Som det er redegjort for i kapittel 4.4 *Hva skal lagres,* er det dessuten snakk om en utvidelse av type data som skal lagres i forhold til gjeldende rett, i tillegg til at denne type lagringsplikt er ny i norsk rett. Innføring av en lagringsplikt av hensyn til kriminalitetsbekjempelse, medfører lagring av svært store mengder opplysninger om lovlydige borgeres legitime kommunikasjon. Når politiet får tilgang til flere opplysningstyper for en lengre periode enn de har i dag, gir dette politiet større mulighet til å følge personer, etablere kontaktnett og bygge profiler enn etter gjeldende rett. Det må kunne legges til grunn at dette vil kunne lette politiets arbeid med å etterforske og bekjempe kriminalitet. Det er samtidig viktig å være klar over den mulige nedkjølende effekten datalagringen kan ha på borgernes vilje til åpen og fri kommunikasjon. Denne nedkjølende effekten vil kunne påvirkes i negativ retning dersom omfanget av de lagrede data er stort, lagringstiden er lang og om dataene er mangelfullt sikret mens de er lagret. Dersom borgerne opplever at deres kommunikasjon ikke er tilstrekkelig vernet, kan dette således få negative konsekvenser for den frie meningsdannelse, som er grunnleggende i et demokrati.

Retten til privat kommunikasjon er vernet i EMK artikkel 10. Det er derfor viktig å velge datalagringsløsninger som på en best mulig måte ivaretar borgernes rett til integritets- og kommunikasjonsvern, samtidig som politiet gis mulighet til å benytte spor fra elektronisk kommunikasjon i sin etterforskning av alvorlige kriminalsaker. Ved valg av lagringstid, må man derfor se på både mengde og type opplysninger som skal lagres. Av hensyn til majoritetens personvern, bør man, basert på opplysningenes omfang, velge det minst inngripende lagringsalternativet. Mengden data som skal lagres, sammenholdt med at implementering av direktivet uansett vil medføre økt lagringstid i forhold til gjeldende rett, taler av personvernhensyn for å velge kortest mulig lagringstid.

Lagringstiden har også innvirkning på kostnadene for lagringen, men er ikke den faktor som er mest kostnadsdrivende. Tilbyderne lagrer data i tre til fem måneder i dag, og en eventuell økning til seks måneder vil ikke gi de store kostnadsmessige utslagene. Sett fra ekommyndighetens ståsted vil heller ikke en lagringstid lengre enn seks måneder være avgjørende for konkurransen i ekommarkedet.
Norske myndigheter har innenfor elektronisk kommunikasjon en tradisjon for å se hen til de andre nordiske land når det gjelder regulering av områdene. Som det redegjøres for i kapittel 3 har både danske og finske myndigheter innført en lagringstid på ett år. Departementene mener like krav til lagringstid i de nordiske landene i utgangspunktet er hensiktsmessig med tanke på politiets samarbeid på tvers av landegrenser og med tanke på at flere tilbydere av ekomnett og -tjenester opererer på et nordisk marked. I og med at Sverige ikke har implementert datalagringsdirektivet ennå veier dette hensynet mindre. Hensynet til at man opererer med et nordisk ekommarked vil uansett ikke alene være avgjørende for norske myndigheters valg av lagringstid.

Norske myndigheter har også merket seg at enkelte land skiller på lagringstid for ulike tjenester. For eksempel har Storbritannia i sin eksisterende bransjebaserte ordning et skille på lagringstid avhengig av tjenestene i den forstand at de har ett års lagringstid på data for fasttelefoni og mobiltelefoni og seks måneders lagringstid for data knyttet til Internettaksess og e-post.

Departementene ønsker i denne omgang ikke å skille på lagringstid etter teknologi dersom det innføres en lagringsplikt i norsk rett. Det er ønskelig med en teknologinøytral regulering innenfor elektronisk kommunikasjon. Det vil si at reguleringen av en tjeneste skal være lik, uavhengig av teknologi eller produksjonsmåte. Ulik lagringstid kan innebære konkurransefordeler for tilbydere av teknologier som får kortere lagringstid enn tilbydere av teknologier som får lengre lagringstid. Datalagringsdirektivet nevner tre former for taletjenester: fasttelefoni, mobiltelefoni og bredbåndstelefoni. Å pålegge ulik lagringstid for disse tjenestene, vil være uheldig, da tilbyderne av disse tjenestene konkurrerer i det samme markedet.

Politimyndighetenes behov har tidligere stort sett knyttet seg til fast- og mobiltelefoni. På slutten av 2005 hadde 16 % av bredbåndskundene på det norske markedet bredbåndstelefoni – første kvartal 2009 hadde andelen steget til 34 %. Utviklingen tyder på at politiets behov, når det gjelder data knyttet til tale og telefonitjenester, også

knytter seg til bredbåndstelefoni, noe som taler for lik lagringstid for forskjellige teknologier.

Allerede nå, og i økende grad i årene som kommer, ser vi flere konvergerende kommunikasjonstjenester. Det vil si hybridtjenester som benytter forskjellige typer teknisk infrastruktur og produksjonsmåte for en og samme tjeneste (for eksempel tale og video). I dag tilbys det tjenester på det norske markedet der mobiltelefoner også kan benyttes som bredbåndstelefon i trådløse soner. En tilbyder av denne type tjenester/abonnement, som av sluttbrukere oppfattes som én tjeneste ville, hvis man valgte ulik lagringstid på ulike teknologier, måtte lagre trafikkdata med to forskjellige lagringstider avhengig av hvordan forbrukeren velger å benytte tjenesten.

Departementene ber særskilt om høringsinstansenes syn på lagringstid og forslaget om ikke å skille på lagringstid etter teknologi.

4.9 **Krav til lagring og levering av lagrede data**

I henhold til datalagringsdirektivet artikkel 8 skal medlemslandene sørge for at de relevante data faktisk lagres i overensstemmelse med lagringsplikten og at lagringen legger til rette for overføring av data uten unødvendige forsinkelser (undue delay)ved anmodning fra kompetent myndighet. Hva som menes med unødvendige forsinkelser vil kunne være et diskusjonsspørsmål. Departementene ønsker ikke å fremme forslag knyttet til krav til overlevering av data eller tidsgrense for hvor raskt dataene skal leveres fra tilbyder til politiet. Det legges til grunn at tilbyderne vil utlevere på den raskeste, økonomisk mest effektive og sikreste måten som er mulig for dem, når politiet etterspør data. Det vises for øvrig til det arbeidet som gjøres med hensyn til standardisering på dette området.

Den tekniske komiteen i TC LI i ETSI (The European Telecommunications Standards Institute) utarbeider standarder for datalagring. Det er inntil nå tre dokumenter som direkte relaterer seg til kravene i direktivet:

- TS 102 656 ”Requirements of LEAs for handling Retained Data”, som inneholder en rekke anbefalinger og krav til hvordan tilbyder skal forholde seg til henvendelser fra myndighetene om utlevering av trafikkdata. Standarden spesifiserer også hvilke data som skal utleveres, jf artikkel 5 i datalagringsdirektivet.
- TS 102 657 ”Handover interface for the request and delivery of Retained Data”, som blant annet beskriver hvilke formater utleverte data skal overleveres i og hvordan den fysiske utleveringen skal skje.
- TR 102 661 V1.1.1 ” Security framework in Lawful Interception and Retained Data environment” som beskriver en rekke sikkerhets- og sårbarhetsaspekter i forbindelse med lagring og håndtering av trafikkdata. Dokumentet gir anbefalinger om hvordan tilbyder ved hjelp av tekniske og administrative metoder kan oppnå et akseptabelt sikkerhetsnivå for lagringsløsninger m.m.

ETSIs standarder og rapporter innenfor dette området er ikke bindende.

Krav til politiets behandling av trafikkdata som er blitt utlevert vil bli regulert av lov om behandling av opplysninger i politiet og påtalemyndigheten - politiregisterloven (Ot.prp.nr. 108 2008-2009). Lovforslaget er i samsvar med rådets rammebeslutning av 27. november 2008, om vern av personopplysninger i forbindelse med politisamarbeid og rettslig samarbeid i straffesaker. Politiregisterloven fastsetter bl.a. bestemmelser om informasjonssikkerhet og kontroll, politiets taushetsplikt, utveksling, regler om retting, sletting og tilsyn.

4.10 **Tilsyn med lagringen**

I henhold til artikkel 9 i direktivet skal medlemslandene gi en eller flere offentlige myndigheter ansvaret for å føre tilsyn med datasikkerheten hos tilbyder.

Departementene foreslår at dersom direktivet skal gjennomføres i norsk rett videreføres dagens tilsynsordning med et delt tilsynsansvar mellom Post- og teletilsynet og Datatilsynet

4.10.1 Tilsyn etter ekomloven

Post- og teletilsynet har et generelt tilsynsansvar etter ekomloven for å sikre at krav fastsatt i eller i medhold av loven oppfylles. Herunder fastsetter ekomloven § 2-7 visse krav til tilbyder for kommunikasjonsvern. Bestemmelsen omhandler nødvendige sikkerhetstiltak til vern av kommunikasjon som overføres via elektroniske kommunikasjonsnett- eller tjenester, og behandling av trafikkdata. Post- og teletilsynet har et sektorspesifikt myndighetsansvar for å føre tilsyn med at tilbyder overholder disse kravene. Det legges opp til en videreføring av gjeldende tilsynsansvar for kommunikasjonsvern.

Post- og teletilsynet er også tilsynsmyndighet når det gjelder tilbyders tilretteleggingsplikt etter gjeldende § 2-8 om tilrettelegging for lovbestemt tilgang til informasjon. Det legges opp til at Post- og teletilsynet også fremover skal ha ansvar for å føre tilsyn med at tilbydere av elektroniske kommunikasjonsnett- og tjenester legger til rette for lovbestemt tilgang til informasjon.

Etter ekomloven § 10-1 har Post- og teletilsynet et generelt tilsynsansvar for at krav fastsatt i eller i medhold av loven er oppfylt. Dette gjelder også for krav om kommunikasjonsvern og tilretteleggingsplikt jf ovenfor. Det legges opp til at Post- og teletilsynet også fremover skal føre tilsyn med at tilbyder faktisk lagrer relevante data dersom den foreslåtte bestemmelsen om lagringsplikt og relaterte forskriftsbestemmelser blir vedtatt. Videre foreslås det at Post- og teletilsynet skal føre

tilsyn med at tilbyderne overholder plikten til å slette data i overensstemmelse med den foreslåtte bestemmelsen om sletteplikt for data som er lagret til formål for kriminalitetsbekjempelse. Ekomlovens § 10-1 innebærer videre at alle som har rettslig interesse i en sak kan bringe spørsmål om en tilbyder har opptrådt i strid med krav i eller i medhold av loven til avgjørelse for myndigheten. Dette betyr at kompetente myndigheter med lovbestemt tilgang til data som det i medhold av loven påhviler tilbyder å lagre kan innbringe spørsmål for Post- og teletilsynet dersom lagringsplikten ikke overholdes. Tilsynet kan der det er berettiget iverksette et eller flere av sanksjonsmidlene som er nevnt i ekomloven kapittel 10.

I tillegg har Post- og teletilsynet et særlig personvernrelatert tilsynsansvar som knyttes opp mot bestemmelsene om tilbyders taushetsplikt i ekomloven § 2-9. Det legges ikke opp til endringer på tilsynsoppgavene til Post- og teletilsynet på dette punktet.

4.10.2 Tilsyn etter personopplysningsloven

Datatilsynet har allerede i dag til oppgave å kontrollere at lover og forskrifter som gjelder for behandling av personopplysninger blir fulgt, jf. personopplysningsloven § 42. Sentralt for tilsynets vurdering vil være om tilbyder oppfyller de krav til informasjonssikkerhet som følger av personopplysningsloven § 13 med tilhørende forskrifter, samt at de øvrige krav til behandling av personopplysningene følges, jf kapittel 6.1 om retten til lagring av data hos tilbyder. Etter personopplysningsloven §§ 46 og 47 har Datatilsynet kompetanse til å ilegge overtredelsesgebyr eller tvangsmulkt dersom behandlingsansvarlig ikke overholder gjeldende personopplysningsregelverk. Departementene mener at det er naturlig å videreføre dette tilsynsansvaret etter personopplysingsloven også for data som lagres i medhold av den foreslåtte bestemmelsen om lagringsplikt. Det legges i utgangspunktet ikke opp til at Datatilsynet skal tillegges en særskilt tilsynskompetanse etter ekomloven. Videre har Datatilsynet etter dagens regelverk et tilsynsansvar når det gjelder tilbyders behandling og sletting av data som er lagret til kommunikasjons- eller faktureringsformål, jf beskrivelsen i avsnitt 6.1 om personopplysningsforskriften § 7-1 og Datatilsynets konsesjoner. Det legges ikke opp til endringer på dette punkt. Datatilsynet vil derfor fortsatt ha ansvar for å føre tilsyn med at behandling og sletting av data som er lagret hos ekomtilbyderne skjer etter gjeldende personopplysningslov, -forskrift og konsesjoner. Tilsynsansvaret gjelder både data lagret i medhold av ekomloven og data lagret i medhold av konsesjoner gitt av Datatilsynet med hjemmel i personopplysningsloven.

Det vil i noen grad være overlappende tilsynskompetanse mellom Post- og teletilsynet og Datatilsynet på deler av dette området. Departementene viser til at det foreligger en avtale mellom Post- og teletilsynet og Datatilsynet for utøvelse av tilsyn. Departementene vil vurdere å be tilsynene styrke denne avtalen dersom det innføres en lagringsplikt.

Departementene ber om høringsinstansenes syn på forslaget om å videreføre det delte tilsynsansvaret mellom Post- og teletilsynet og Datatilsynet.

4.11 **Statistikk**

Det fremgår av datalagringsdirektivets artikkel 10 at medlemslandene er forpliktet til årlig å sende inn statistikk til EU-kommisjonen om datalagringen. Ved en eventuell implementering av datalagringsdirektivet i norsk lov forplikter norske myndigheter seg tilsvarende til å sørge for årlig statistikk til ESA om datalagring. Det skal i henhold til direktivet føres statistikk om antall saker hvor anmodninger blir imøtekommet, tiden mellom lagringstidspunkt (dato) og etterspørsel etter data og saker der anmodning om data ikke har blitt imøtekommet. I og med at implementeringen av direktivet vil være med referanse til vedlegg 11 om telekommunikasjon i EØS-avtalen, finner departementene det naturlig at det er Post- og teletilsynet som får ansvaret for å oversende denne statistikken til ESA. Andre lands myndigheter, som for eksempel Storbritannia, legger opp til at det er tilbyderne som skal føre statistikken over datalagringen. Departementene kan ikke se at det foreligger særskilte grunner for å pålegge ekomtilbyderne en plikt til å utarbeide eller rapportere egen statistikk, og foreslår derfor at det er politiet og andre myndigheter som anmoder om data som må føre statistikken og videresende denne til Post- og teletilsynet for oversendelse til ESA. EU-kommisjonen har utarbeidet et skjema for hva og hvordan slik statistikk skal føres. Tanken er at det skal være ensartet rapportering for alle EUs medlemsstater. Det vil være naturlig for EØS-landene å benytte samme format, men dette vil det være opp til ESA å beslutte.

4.12 **Politiets tilgang til data**

Adgangen til å hente ut data som er lagret i henhold til datalagringsdirektivet, er regulert i direktivet artikkel 4 som lyder (dansk oversettelse):

”Medlemsstaterne træffer foranstaltninger til at sikre, at data, der lagres i overensstemmelse med dette direktiv, kun udleveres til de kompetente nationale myndigheder i særlige sager og i overensstemmelse med national lovgivning. Hver medlemsstat fastsætter i sin nationale lovgivning den procedure, der skal følges, og de betingelser, der skal være opfyldt for at få adgang til lagrede data i overensstemmelse med kravet om nødvendighed og proportionalitet, under hensyn til de relevante bestemmelser i EU-retten og folkeretten, herunder navnlig den europæiske menneskerettighedskonvention, således som den er fortolket af Den Europæiske Menneskerettighedsdomstol.”

Adgang til disse dataene skal følgelig bare kunne gis til visse myndigheter, og det er opp til hver enkelt stat å bestemme hvilke myndigheter som er kompetente til å få data. Et sentralt formål med direktivet er å bekjempe kriminalitet. Det er en oppgave for politi og påtalemyndighet og det må således være riktig at data kan gis til disse.

Direktivet kan likevel neppe forstås som å være til hinder for at også andre myndigheter gis tilgang, for eksempel Toll- og avgiftsetaten eller Skatteetaten.

Departementene vurderer at det er nødvendig at politi og påtalemyndighet gis tilgang til denne informasjonen, men at det også er tilstrekkelig. Ved mistanke om lovbrudd vil andre myndigheter på linje med private kunne anmelde straffbare forhold til politiet som så avgjør om etterforskning skal iverksettes og eventuelt hvilke etterforskningsskritt som skal tas. Vi minner om at det heller ikke i dag er adgang for andre myndigheter enn politiet til å bruke tvangsmidler etter straffeprosessloven som ledd i en straffesak.

Det fremgår videre av datalagringsdirektivet artikkel 4 at lagret data bare skal utleveres i særlige saker. Dette må tolkes i sammenheng med artikkel 1 nr. 1 om at dataene skal være tilgjengelige for bekjempelse av grov kriminalitet. Det er opp til hvert enkelt land å fastsette hva som anses som grov kriminalitet som gir adgang til utlevering av data. Samtidig er det departementenes syn at direktivets formål ikke kan forstås som en uttømmende angivelse av hvordan begrepet "særlige saker" i artikkel 4 skal forstås. Også saker om lovbrudd som det er særlig vanskelig å etterforske uten tilgang til data, må kunne falle inn under begrepet.

Reglene om beslag og utleveringspålegg i straffeprosessloven kapittel 16 gjelder i utgangspunktet alle straffbare forhold. På bakgrunn av departementenes forståelse av kriteriet særlige grunner og direktivets formål om å bekjempe grov kriminalitet, må således reglene om utleveringspålegg endres for å imøtekomme forutsetningen i direktivet om at dette ikke skal gjelde i alle saker.

Det foreslås at utlevering av data bør kunne pålegges dersom det straffbare forholdet har en strafferamme på fengsel i 3 år eller mer. Dette er i samsvar med den definisjonen av alvorlig kriminalitet som er nedfelt i Den europeiske arrestordre 13. juni 2002 (2002/584/RIA). Denne standarden er også anvendt i andre sammenhenger (Rammebeslutning 2006/960 av 18. desember 2006, om forenkling av utvekslingen av opplysninger og etterretninger mellom medlemsstatenes rettshåndhevende myndigheter). Det innebærer en betydelig skjerpelse i forhold til hovedregelen i straffeprosessloven § 210 om at påtalemyndigheten kan pålegge besitteren å utlevere ting som antas å ha bevisverdi i en straffesak. Samtidig settes grensen lavere enn i straffeprosessloven § 216 b om bl.a. kommunikasjonskontroll i sanntid og fremtid. Det regnes som ekstraordinære etterforskningsmidler og det er således naturlig at et mindre inngripende tvangsmiddel har lavere terskel.

Visse forbrytelser som har en lavere strafferamme enn tre år kan være særlig vanskelige å etterforske uten å kunne benytte data. Det er således departementenes syn at også andre saker kan vurderes som "særlige saker". Det gjelder for det første spionasje som rammes av straffeloven §§ 91 og 91 a og terrorvirksomhet som rammes av straffeloven § 104 a. Data er dessuten særlig viktig i etterforskningen av overtredelser av straffeloven § 132 b som gjelder brudd på taushetsplikt ilagt av retten i forbindelse med benyttede tvangsmidler som ransaking eller beslag. Åpenbaring av slik

informasjon vil kunne ødelegge effekten av det aktuelle tvangsmidlet. Datakriminalitet rammes av straffeloven § 145 annet ledd som retter seg mot uberettiget tilgang til data eller programutrustning som er lagret eller som overføres ved elektroniske eller andre tekniske hjelpemidler. Bestemmelsen kom inn i lovgivningen som et ledd i kampen mot datakriminalitet og foreslås også inntatt i oppregningen over straffebud hvor data kan være av særlig stor betydning for etterforskningen. Begrunnet i det særlige behovet for data til bruk i etterforskningen av brudd på straffeloven § 145 a om telefonavlytting, straffeloven § 162 om narkotikalovbrudd, straffeloven § 317 om hvitvasking samt straffeloven § 390 a om forstyrrelse av privatlivets fred, er også disse forbrytelsene inntatt i oppregningen. Endelig vil data kunne være viktige i etterforskningen av enkelte seksuallovbrudd mot barn. Det er straffeloven § 201 a om forberedelse til seksuelle overgrep mot barn (grooming), straffeloven § 203 om kjøp av seksuelle tjenester av personer under 18 år og straffeloven § 204 a om barnepornografi. Departementene ber spesielt om høringsinstansenes syn på denne oppregningen av lovbrudd som er foreslått som alternativer til det generelle kravet om at handlingen skal kunne medføre fengsel i 3 år eller mer.

Data skal utleveres i samsvar med nasjonal lovgivning, jf. artikkel 4. Bestemmelsen stiller ingen ytterligere krav til nasjonal lovgivning. Det er likevel departementenes syn at det er viktig å bidra til rettssikkerhet på dette punktet. Det foreslås derfor at kun retten skal kunne pålegge besitteren å utlevere data. Dette innebærer en skjerpelse i forhold til gjeldende rett hvor utlevering også kan besluttes av påtalemyndigheten etter straffeprosessloven § 205 første ledd første punktum jf. ovenfor under kapittel 2.4.2. Lovforslaget er ment å regulere uttømmende adgangen til utlevering av data. Det vil således ikke lenger kunne skje ved beslutning av påtalemyndigheten etter disse bestemmelsene i straffeprosessloven. Denne endringen innebærer etter departementenes syn at det ikke lenger vil være aktuelt å innhente Post- og teletilsynets forutgående vurdering av spørsmålet om fritak fra taushetsplikten, jf. straffeprosessloven §§ 204 og 210 jf. § 118 som behandles nærmere under punkt 4.13.

En ytterligere skjerpelse i forhold til dagens rettstilstand er foreslått ved innføringen av kravet om at politiet må godtgjøre at "noen med skjellig grunn mistenkes". Til sammenligning er det i dag tilstrekkelig for beslag og utleveringspålegg etter straffeprosessloven kapittel 16 at dataene "antas å ha betydning som bevis". Dette skal riktignok forstås slik at det må foreligge skjellig grunn til mistanke om en straffbar handling, men ikke at en bestemt person skal være mistenkt, jf. kapittel 2.4.2. En konsekvens av lovforslaget på dette punktet, er at politiet ikke lenger vil kunne få tilgang til data der det ikke lar seg bevise at det foreligger skjellig grunn til mistanke som knytter seg til en bestemt person. I den grad dette utgjør et hinder i praksis, medfører innføringen at dette vilkåret av data vil kunne uthentes i færre saker. Det kan igjen føre til at muligheten for å realisere formålet med lagringsplikten – å bekjempe alvorlig kriminalitet – blir noe forfeilet.

Et annet alternativ kunne vært å lovfeste kravet til skjellig grunn, men ikke at dette må knytte seg til noen konkret person. Denne varianten kan gjenfinnes i for eksempel straffeprosessloven § 202 a om skjult fjernsynsovervåkning, men da slik at det i tillegg

kreves at dette tvangsmidlet vil være av vesentlig betydning for etterforskningen. Dette alternativet har imidlertid visse personvernmessige konsekvenser. Lagringsplikten innebærer at tilfanget av data øker både i omfang og tid. Åpnes det dessuten for at politiet skal få utlevert data uten å måtte knytte mistanken til en konkret person, vil samtidig politiets tilgang til overskuddsinformasjon øke tilsvarende.

Departementene ber på denne bakgrunn spesielt om høringsinstansenes syn på utformingen av dette vilkåret.

Artikkel 4 krever også at data bare skal utleveres i den grad det samsvarer med kravet til nødvendighet og proporsjonalitet. Det legges til grunn at straffeprosessloven § 170a som gjelder generelt for all bruk av tvangsmidler i straffeprosessloven, oppfyller dette kravet.

Endelig stilles det krav til at reglene om utlevering skal være i samsvar med Den europeiske menneskerettighetskonvensjonen. Departementene legger til grunn at direktivet ikke er i strid med EMK artikkel 8, jf. kapittel 4.2. Lovforslaget om utleveringspålegg er utformet i samsvar med direktivet artikkel 4. Etter departementenes syn tar utleveringsbestemmelsen høyde for at utlevering ikke skal skje i større grad enn det som følger av nødvendighetskriteriet i EMK artikkel 8 og viser til nærmere drøftelse av denne problemstillingen under kapittel 4.2.

4.13 **Andre myndigheters tilgang til data**

Ifølge direktivet er det bare kompetente nasjonale myndigheter som i overensstemmelse med nasjonal lovgivning i særlige tilfelle skal ha tilgang til de data som omfattes av lagringsplikten. Formålet med direktivet er at dataene skal gjøres tilgjengelige for de ansvarlige myndigheter i forbindelse med etterforskning, oppklaring og rettsforfølgelse av alvorlig kriminalitet. Som nevnt ovenfor under punkt 4.12 går departementene inn for at det kun er politiet som skal ha adgang til tvangsmidler som ledd i etterforskning av straffbare forhold.

Som nevnt ovenfor i kapittel 2.6 har Kredittilsynet etter dagens regelverk en hjemmel i verdipapirhandelsloven for innhenting av "trafikkdata" der det foreligger mistanke om visse straffbare brudd på loven. Dersom datalagringsdirektivet innføres i norsk rett, vil det medføre at tilbydere vil lagre økt mengde data over lengre tid enn i dag. Kredittilsynet vil følgelig få utvidet sin tilgang til trafikkdata. Det kan reises spørsmål om hvor hensiktsmessig dette er. Departementene gjør videre oppmerksom på at regelverket for Kredittilsynets tilgang ikke forutsetter at retten har truffet avgjørelse om utlevering slik det nå foreslås for politiets tilgang til data. Det kan derfor stilles spørsmål ved hvordan Kredittilsynes tilgang til trafikkdata passer inn i det regime som vil gjelde for politiets tilgang ved innføring av regler som foreslått i dette høringsnotatet.

Departementene ber spesielt om høringsinstansenes syn på dette.

4.14 **Post- og teletilsynets rolle**

Det vises til de foreslåtte endringer i straffeprosessloven som innebærer at politiets innhenting av data bare skal kunne kan skje på grunnlag av utleveringspålegg fra retten. Departementene mener at rettens behandling av slike saker kan sies å overflødiggjøre Post- og teletilsynets forutgående vurdering av spørsmålet om fritak fra taushetsplikt som rettsikkerhetsgaranti. Det vil også være i samsvar med Metodekontrollutvalgets forslag, jf. nærmere omtale ovenfor under punkt 2.4.4. Trolig er den rimelighetsvurderingen tilsynet foretar med grunnlag i straffeprosessloven § 118 første ledd siste punktum, hovedsaklig sammenfallende med den forholdsmessighetsvurderingen som følger av straffeprosessloven § 170 a og som retten vil foreta ved kjennelse om utlevering. På denne bakgrunn foreslås at Post- og teletilsynet løses fra oppgaven med å frita tilbyder fra taushetsplikten når retten har besluttet at data skal utleveres.

Endringen foreslås gjennomført ved endring av bestemmelsen i ekomloven § 2-9, som omhandler tilbyders taushetsplikt og de unntak som gjelder for denne. Departementene ber om synspunkter på forslag til en ny bestemmelse i ekomloven § 2-9 femte ledd om at tilbyders taushetsplikt heller ikke er til hinder for at data utleveres til påtalemyndigheten eller politiet når retten har truffet kjennelse etter reglene i straffeprosessloven kapittel 16 om beslag og utleveringspålegg, jf. lovutkastet. Bestemmelsen vil innebære at Post- og teletilsynet fremover ikke – slik det er tilfelle i dag – vil foreta en vurdering av om det i de enkelte tilfelle er grunnlag for å oppheve tilbyders taushetsplikt etter § 2-9 slik at data kan utleveres til politi eller påtalemyndighet. Det vil etter lovforslaget være opp til retten alene å vurdere når vilkårene for utlevering er til stede.

Et unntak fra taushetsplikten slik som her er antydet innebærer ingen opphevelse av taushetsplikten i andre tilfeller enn de som er nevnt i unntaket, herunder tilfeller der andre myndigheter har lovlig tilgang til trafikkdata, se avsnitt 4.12. I slike andre tilfeller som ikke omfattes av unntaket vil Post- og teletilsynet fortsatt ha en rolle når det gjelder å frita tilbyder fra taushetsplikten. Dette gjelder også i saker om bevisføring etter tvisteloven § 22-3.

Departementene ber om høringsinstansenes syn. Særlig ønsker vi instansenes syn på om Post- og teletilsynet fortsatt bør ha en rolle i sakene om politiets tilgang til data for etterforskning og forebygging av alvorlig kriminalitet.

5. FORHOLDET TIL KILDEVERNET

Kildevernet – pressens rett til å beskytte sine kilder – foreslås ikke endret. Fra pressehold er det tidligere tatt til ordet for at det bør gjelde et generelt forbud mot etterforskning som retter seg mot hvem som er kilder til opplysninger i konkrete saker. Et slikt forbud ville bety at politiet heller ikke kan søke å finne kilden om det brukes andre fremgangsmåter enn spørsmål til ansatte i pressen eller beslag av redaksjonelt

materiale. Problemstillingen er omtalt i Ot. prp. nr. 55 (1997-1998) Om lov om endringer i rettergangslovene m.m. (kildevern og offentlighet i rettspleien) punkt 3.4. på side 40:

"Departementet anser det klart at en slik regel ikke har noe for seg når kilden selv har begått straffbare handlinger. Både når vedkommende har gitt taushetsbelagte opplysninger og når vedkommende som anonym kilde har gitt opplysninger om sine egne straffbare handlinger, må det kunne foretas etterforskning når dette skjer uten å kreve at mediearbeidere oppgir kilden i strid med kildevernet.

I andre tilfelle har det interesse for etterforskningen i en straffesak å finne frem til en anonym kilde som mulig vitne i saken. Et forbud som foreslått vil være til hinder for dette, også i en situasjon hvor man har søkt etter vitnet allerede før vedkommende gikk til pressen. Et forbud vil derfor åpne mulighet for at mulige vitner kan unndra seg sin vitneplikt. Så langt det gjeldende kildevern strekker seg, er kilden beskyttet mot at pressen pålegges å oppgi hans navn, og mot at identiteten ellers røpes ved ransaking eller beslag hos pressen. Ut fra dette kan vedkommende ha den ønskede tillit til pressen. Departementet kan ikke se at dette tillitsforholdet – som det ut fra samfunnsmessige hensyn er ønskelig å opprettholde – blir nevneverdig rokket ved å fastholde adgangen til å etterforske saken på annen måte enn ved vitnepålegg, ransaking og beslag mot pressen."

Beslag av data vil være aktuelt i etterforskningen av et mulig straffbart forhold der de nærmere vilkårene for slikt beslag er oppfylt. Departementene har ikke inngående kjennskap til i hvilke situasjoner det kan være aktuelt med etterforskning som tar sikte på å avdekke pressens kilder. Det typiske vil muligens være at det er kilden som er mistenkt for en straffbar handling, for eksempel for straffbart brudd på taushetsplikt. I utgangspunktet synes det således å være avgjørende at det i de tilfellene vi her taler om er *tilbyder* og ikke den ansatte i pressen som *besitter* de aktuelle dataene som politiet ønsker innsyn i, og at det er hos tilbyder beslaget skjer. Det synes derfor nærliggende å trekke den konklusjonen at kildevernet i utgangspunktet ikke vil medføre noen begrensinger i beslagsadgangen hos tilbyder.

På den annen side må det være klart at beslag som hovedregel vil være utelukket der dataene er i *pressens besittelse* og beslaget foregår hos journalisten eller i redaksjonslokalet, jf. straffeprosessloven § 210 første ledd første punktum som foreskriver at utleveringspålegg bare kan finne sted i den utstrekning det foreligger vitneplikt. Pressens fritak fra vitneplikten er nedfelt i straffeprosessloven § 125.

Det kan trolig stilles spørsmål ved hvor langt begrensingene i adgangen til å ta beslag rekker i tilfeller der journalisten er den mistenkte. I Rt. 2000 side 531 har Høyesteretts kjæremålsutvalg lagt til grunn at begrensingene også skal gjelde der vedkommende journalist er siktet i saken. Avgjørelsen er imidlertid kritisert av Andenæs som mener at det riktige må være at straffeprosessloven § 204 på samme måte som straffeprosessloven § 125, bare gjelder overfor en journalist som er vitne, jf. Tor-Geir Myhrer : Andenæs Norsk straffeprosess 4. utg. (2009) på side 321.

Selv om en innføring av datalagringsdirektivet vil kunne medføre enkelte utfordringer for kildevernet, mener departementene før høringen at det ikke vil innebære uforholdsmessige inngrep. Departementene ser at spørsmålet kan problematiseres, og ber om høringsinstansenes syn på dette.

6. ADMINISTRATIVE OG ØKONOMISKE KONSEKVENSER

Datalagringsdirektivet innehar ingen bestemmelser om kostnader. Departementene er imidlertid kjent med at det har pågått og pågår debatter i de fleste av EUs medlemsland om hvem som skal dekke kostnadene knyttet til lagringen. Det ligger an til at land velger ulike modeller også innenfor Norden. I Danmark må tilbyderne dekke merkostnadene som følge av lagringsplikten selv, mens politiet betaler for uthenting. I Finland vil alle merkostnadene bli dekket av justismyndighetene.
Dagens kostnadsmodell i Norge når det gjelder lovbestemt tilgang til informasjon, er en delingsmodell hvor ekomtilbyderne har en tilretteleggingsplikt og forutsettes å dekke kostnadene knyttet til denne plikten. Tilbydernes driftskostnader/uthentingskostnader dekkes av politiet i henhold til avtaler jf. ekomloven § 2-8, andre ledd. Det legges i denne omgang ikke opp til noe forslag om å endre dagens kostnadsmodell. Dersom datalagringsdirektivet innføres i norsk rett foreslår departementene at det fortsatt skal være en delingsmodell hvor ekomtilbyderne har en tilretteleggingsplikt og dekker kostnadene til denne plikten, mens drifts/uthentingskostnader dekkes av politiet i henhold til avtaler.

Kostnadsbildet vil ved innføring av en lagringsplikt kunne bli noe annerledes enn i dag. Det er snakk om data som tilbyderne vil bli pålagt å lagre og som de med stor sannsynlighet vil måtte etablere egne systemer for. Avhengig av hvorvidt tilbyderne lagrer data i dag eller ikke vil de på grunn av økt volum og lengre lagringstid måtte tilpasse etablerte systemer eller etablere nye systemer for lagring. Teleplans utredning og ekombransjen har gitt uttrykk for at det som koster når det gjelder datalagring er å etablere systemer for lagring og for uthenting av data. Det må også kunne forventes noe økte kostnader knyttet til sikkerhet. Kostnaden per sak vil kunne komme til å gå opp. Kostnader for å få systemene på plass (investeringer) vil påløpe for alle tilbyderne og det samme vil driftskostnader, sistnevnte i varierende grad avhengig av hvor stor etterspørselen fra politiet er. Det er flere faktorer som gjør det vanskelig å si eksakt hva kostnadene knyttet til lagringsplikten vil bli. Variasjonen er stor blant tilbyderne både mht. hvilke tjenester de tilbyr og hvilke tekniske systemer de benytter i dag. To tilbydere som tilsynelatende er like mht innhold og størrelse kan ha så ulike tekniske systemer at kostnadsanslagene blir totalt ulike.

Som nevnt i kapittel 5 gjorde Teleplan i 2007/2998 en utredning som viser en beregning av kostnader for alle tilbydere av elektroniske kommunikasjonsnett og -tjenester ved en eventuell innføring av datalagringsdirektivet. Analysen viser at det totalt vil koste mellom 207 og 261 MNOK over en femårsperiode for seks måneders lagring, avhengig av hardwareløsninger og hvor mye tilpasninger som kreves til tilbydernes systemer.

Den laveste kostnaden forutsetter en enkel hardwareløsning hvor hardware ikke er duplisert, slik at løsningen ikke er så robust dersom feilsituasjoner inntreffer. Det forutsettes også at det i liten grad er nødvendig med tilpasning til tilbyders systemer. Den høyeste kostnaden forutsetter at det kreves robust hardwareløsning med duplikasjon og stor grad av tilpasninger til tilbyders systemer slik at software og prosjektkostnader er høye.

Det fremgår også av Teleplans analyse at dersom alle små tilbyderne utvikler en enkel løsning som kan gjenbrukes, med lokale tilpasninger hos hver enkelt tilbyder, vil man kunne få en kostnadsreduksjon på ca 40 MNOK. Det er ikke gjort noen kartlegging av om en slik løsning ville bli benyttet av tilbyderne, men for tilbydere som ikke har lagringsløsninger i dag kan det være en løsning dersom det gir kostnadsmessige besparelser i forhold til å utvikle en egen løsning. Av analysen fremgår det ikke hvilken kostnadsreduksjon som kan ventes dersom også mellomstore og store tilbydere utvikler løsninger som kan gjenbrukes.

Teleplans analyse viser videre at lagringstid i liten grad påvirker kostnadene for lagring. Hvis man øker lagringstiden fra 6 måneder til 12 måneder gir det en marginal økning i kostnader. Informasjonssikkerhet virker til en viss grad inn på kostnadene. Det fremgår blant annet av analysen at dersom det stilles samme krav til lagring av dataene som det gjøres i dag, er ikke informasjonssikkerheten en betydelig kostnad for tilbydere som allerede lagrer. For tilbydere som ikke lagrer vil det måtte påregnes kostnader forbundet med etablering av rutiner og infrastruktur som kreves for sikker og god behandling av personopplysninger. Noen tilbydere ser for seg å opprette en separat løsning for lagring av data, andre ser for seg å benytte dagens løsning som brukes for fakturering og bare utvide lagringstiden. Ettersom noen ser for seg å benytte løsningen de allerede har, er det noen tilbydere som antar at de ikke vil ha behov for å investere i nye løsninger da kapasiteten er god nok i eksisterende systemer.

Det er viktig å understreke at det i Teleplans analyse ikke er tatt høyde for at flere av tilbyderne, og da særlig de store tilbyderne (infrastruktureierne), allerede har systemer for lagring. Analysen sier heller ikke noe om fordelingen av kostnader mellom politiet og tilbyderne, jf avsnittet over om dagens kostnadsdeling. Teleplan peker gjentatte ganger på at det i analysen er snakk om grove estimater og at det er vanskelig å få et korrekt kostnadsbilde så lenge tilbyderne ikke vet eksakt hvilke krav de eventuelt vil bli stilt overfor ved innføring av datalagringsdirektivet. Departementene erkjenner at dette er en utfordring. Det er følgelig departementenes oppfatning at tallene fra Teleplans analyse ikke gir et tilstrekkelig godt grunnlag for beregning av de økonomiske og administrative konsekvensene, og det vil derfor være nødvendig å foreta ytterligere vurderinger av dette.

Dersom datalagringsdirektivet gjennomføres i norsk rett må det forventes at både Post- og teletilsynet og Datatilsynet får økte tilsynsforpliktelser, og følgelig økte administrative kostnader. Post- og teletilsynet finansierer sin virksomhet gjennom gebyrer fra tilbydere av ekomnett og -tjenester, mens Datatilsynet ikke har tilsvarende

mulighet for å få dekket de eventuelle økte kostnadene knyttet til økte tilsynsforpliktelser.

7. MERKNADER TIL DE ENKELTE BESTEMMELSER I LOV- OG FORSKRIFTSFORSLAGET

Til straffeprosessloven § 210 første ledd nytt annet punktum

Første ledd nytt annet punkt gjelder utlevering av historiske data fremkommet ved bruk av elektronisk kommunikasjon og vil således gå foran første punktum for så vidt gjelder slike ting. Som data regnes bl.a. opplysninger om hvilke telefoner som har vært i kontakt, samt når og hvor lenge samtalen varte. Data omfatter også internett-telefoni og e-postutveksling, samt utlevering av alle data i et bestemt geografisk område, for eksempel et bysentrum eller en bydel. Data vil etter dette ikke kunne beslaglegges eller besluttes beslaglagt i medhold av straffeprosessloven § 205, eller begjæres utlevert i medhold av straffeprosessloven § 210 første ledd første punktum.

Bestemmelsen gjelder all utlevering av data som er lagringspliktig i medhold av e-komloven § 2-8 annet ledd men er ikke begrenset til utlevering av slik data. Den vil således også komme til anvendelse på trafikkdata som er lagret av kommersielle årsaker. Trafikk som skjer nå eller som antas å finne sted i fremtiden, skal fortsatt reguleres av straffeprosessloven § 216 b.

Bestemmelsen er noe strengere enn første punktum idet det her knesettes et krav om "noen med skjellig grunn mistenkes". I den grad politi og påtalemyndighet har behov for slik data i avvergelsesøyemed, gjelder straffeprosessloven § 222 d.

Den handlingen som kan gi grunnlag for et utleveringspålegg, må ha en strafferamme på fengsel i 3 år eller mer. Alternativt må forholdet omfattes av en av nærmere angitte straffebestemmelser. Oppregningen her er uttømmende. Disse lovbruddene kjennetegnes ved at data antas å være et særlig effektivt tvangsmiddel i etterforskningen.

I forhold til data som er lagringspliktig i medhold av e-komloven § 2-8 annet ledd, settes yttergrensen for hva slags data som besitteren kan pålegges å utlevere, av *hva* som er omfattet av lagringsplikten samt underlagt sletteplikten i e-komloven § 2-7 annet ledd. Det vises til nærmere omtale av denne bestemmelsen under kapittel 4.11.

Til ekomloven § 2-7 annet ledd

Bestemmelsen fastsetter hovedregelen om sletteplikt for trafikkdata, lokaliseringsdata og data nødvendig for å identifisere abonnenten eller brukeren. Bestemmelsen er en utvidelse av gjeldene bestemmelse i § 2-7 annet ledd om behandling av trafikkdata. Utvidelsen synliggjør at sletteplikten også gjelder for lokaliseringsdata som ikke er

trafikkdata. Utvidelsen gjelder også for data nødvendig for å identifisere abonnenten eller brukeren når slike data ikke er nødvendig av kommunikasjons- eller faktureringsformål. Denne reservasjonen medfører blant annet at sletteplikten ikke gjelder for telefonnummer, og faste IP-adresser. Telefonnummer og faste IP-adresser er eksempler på identifiseringsdata som er nødvendig både for kommunikasjonsformål og/eller for faktureringsformål. Slike data vil i realiteten derfor ikke være omfattet av sletteplikten.

Bestemmelsens ordlyd foreslås også endret som en konsekvens av innføring av lagringsplikten. Dette innebærer at tilbyder fremover vil lagre data til to forskjellige formål. Endringen innebærer ingen realitetsendring i forhold til tidspunkt for sletting av data som er lagret til kommunikasjons- eller faktureringsformål. Slike data vil fortsatt skulle slettes når kommunikasjons- eller faktureringsformål ikke lenger er til stede. Data som er lagret for å legge til rette for etterforskning og rettsforfølgning av alvorlige straffbare forhold, skal slettes samtidig med at lagringsplikten opphører. Bestemmelsen i § 2-7 tredje ledd går således foran bestemmelsen i personopplysningsloven § 28 om sletteplikt.

Til ekomloven § 2-8 nytt annet ledd

Bestemmelsen er ny, og innfører lagringsplikt i en periode på X måneder for visse typer data. Innføring av en lagringsplikt skal sikre at definerte data skal være tilgjengelige for relevante myndigheter i forbindelse med oppklaring, etterforskning og rettsforfølgelse av alvorlig kriminalitet.

Data som foreslås lagret er trafikkdata, lokaliseringsdata og andre data som genereres eller fremkommer i tilbyders elektroniske kommunikasjonsnett ved bruk av fasttelefoni, mobiltelefoni, internettelefoni, internettaksess og e-post, og som er nødvendig for å identifisere abonnenten eller brukeren. For nærmere forståelse av begrepene trafikkdata og lokaliseringsdata vises til merknaden til § 2-7. Lagringsplikten gjelder data som er nødvendig for å spore og identifisere kilder til en kommunikasjon, destinasjonen og typen av en kommunikasjon, dato, tid og varighet for en kommunikasjon samt for å identifisere brukers kommunikasjonsutstyr og lokaliseringen av mobilt terminalutstyr. Når det gjelder begrepet "mobilt terminalutstyr" er "terminalutstyr" allerede definert i gjeldende ekomlov § 1-5. I de tilfelle det er snakk om mobilt terminalutstyr vil det ved lokaliseringen av utstyret være relevant å fastslå det nærmeste faste punktet som terminalutstyret er tilknyttet ved et gitt tidspunkt. Dette vil typisk være en antenne, for eksempel en basestasjon, et trådløst aksesspunkt og lignende. Det er den geografiske posisjonen til disse antennene som vil identifisere lokaliseringen av terminalutstyret.

For *fasttelefoni* skal følgende lagres: A-nummer, dvs. oppringers telefonnummer. B-nummer, dvs. telefonnummer til den som blir oppringt. C-nummer, dvs. telefonnummer til videresendt abonnement. Abonnent/brukerdata og registrert bruker/identitet for eier av A, B og C nummer. Dato og tidspunkt ved start og avslutning av kommunikasjon. Ved *mobiltelefoni* skal A-nummer, B-nummer, C-nummer, de

internasjonale IMEI/IMSI identiteter for A- B- og C- nummer, og abonnent/brukerdata og registrert bruker/identitet for eier av A, B og C nummer, lagres. I tillegg skal dato og tidspunkt ved start og avslutning av kommunikasjon, informasjon om hvilken kommunikasjonstjeneste som er benyttetog lokaliseringsinformasjon ved start og avslutning av kommunikasjon, lagres. Ved *bredbåndstelefoni* skal følgende data lagres; IP-adresser som identifiserer oppringer og den som blir oppringt, tildelt brukeridentitet, navn og adresse til abonnent eller registrert bruker som IP-adresse eller/og telefonnummer ved oppringt tjeneste, brukeridentitet eller telefonnummer som tildeles den eller de som er mottaker av en bredbåndstelefonisamtale og informasjon som identifiserer kommunikasjonsutstyr eller kommunikasjonsanlegg. Ved *internettaksess* skal følgende data lagres: brukers IP-adresse, abonnentinformasjon, registrert brukerinformasjon, dato og tidspunkt for pålogging og avlogging av internettjenesten, type internettoppkobling og informasjon som identifiserer kommunikasjonsutstyr eller kommunikasjonsanlegg. Ved *e-post* skal følgende data lagres, avsender og mottakers e-postadresse og IP-adresser, abonnentinformasjon og registrert brukerinformasjon og dato og tidspunkt for pålogging og avlogging til e-posttjenesten.

Innhold, eller noe som avslører innhold i kommunikasjonen, omfattes ikke av tilbyders lagringsplikt. Forslag til ny bestemmelsen regulerer heller ikke forhold vedrørende utlevering av data. Utlevering reguleres blant annet av § 2-9 og av straffeprosesslovens regler. Lagringsplikten opphører etter X måneder, og avløses som utgangspunkt av sletteplikt i medhold av § 2-7 annet ledd.

Plikten til å lagre vil gjelde for enhver fysisk eller juridisk person som tilbyr andre tilgang til elektronisk kommunikasjonsnett som anvendes til offentlig elektronisk kommunikasjonstjeneste eller tilbyder av slik tjeneste. Når det gjelder tilbyderbegrepet vises til definisjonene i § 1-5, der det fremgår at en tilbyder er "enhver fysisk eller juridisk person som tilbyr andre tilgang til elektronisk kommunikasjonsnett eller –tjeneste". Av definisjonene i § 1-5 fremgår det at elektronisk kommunikasjonstjeneste er "tjeneste som helt eller i det vesentlige omfatter formidling av elektronisk kommunikasjon og som normalt ytes mot vederlag".

Når det gjelder offentlighetsbegrepet er det etter ekomlovens definisjon avgjørende om tjenesten er tilgjengelig for allmennheten eller beregnet til bruk for allmennheten, jvf. § 1-5, nr 7. Ved vurderingen av om tjenesten tilbys allmennheten, skal det blant annet legges vekt på antall brukere og interessefellesskapet mellom disse. Det legges til grunn at for eksempel borettslag med private nett i denne sammenheng i utgangspunktet ikke vil være omfattet av dette tilbyderbegrepet. Andre eksempler på virksomheter som i utgangspunktet i denne sammenheng er tenkt å falle utenfor er bedrifter, sykehus, hoteller og lignende som utelukkende stiller elektroniske kommunikasjonstjenester til rådighet for sine kunder eller ansatte. Det fremgår av annet punktum at data som skal lagres er data knyttet til fasttelefoni, mobiltelefoni, internettelefoni, internettaksess og e-post. I grensetilfeller vil myndigheten etter ekomloven kunne avgjøre om det er snakk om en offentlig tjeneste som omfattes av lagringsplikten. Dette kan særlig være relevant for tjenester som omfatter web-basert e-post og andre web-baserte applikasjoner. Det vises dessuten til at myndigheten i

henhold til tredje ledd, vil få en relativt vid kompetanse til i særlige tilfeller å kunne frita tilbydere fra plikten til å lagre data, eller pålegge andre enn de som omfattes av andre ledd plikt til å lagre data dersom dette må til for å oppnå formålet med bestemmelsen.

Det vil gå en grense for lagringsplikten. For en tilbyder av fasttelefoni og mobiltelefoni vil ansvaret for lagring stoppe ved et eventuelt samtrafikkpunkt. Tilbyderen må imidlertid kunne gi informasjon om hvem samtrafikkpartneren er.

Til ekomloven § 2-8 nytt fjerde ledd

Det foreslås for det første en videreføring av gjeldende bestemmelse i § 2-8 tredje ledd om myndighetens adgang til å gi forskrift om tilretteleggingsplikt, herunder plikt til å lagre trafikkdata. For det andre foreslås en utvidelse av regelen slik at myndigheten også kan fatte enkeltvedtak der dette er hensiktsmessig. For det tredje foreslås myndigheten gitt hjemmel til å kunne forvalte lagringsplikten slik at den virker etter sin hensikt. Det legges her opp til at myndigheten i særlige tilfelle kan frita tilbydere som omfattes av tilbyderbegrepet i tredje ledd fra lagringsplikten eller pålegge andre en hel eller delvis lagringsplikt. Sist nevnte kan i særlige tilfelle tenkes relevant for nødvendig oppfyllelse av det hensyn som ligger til grunn for innførsel av lagringsplikt. Ved vurderingen om det skal fritas fra lagringsplikten eller om andre enn de som omfattes av tilbyderbegrepet i tredje ledd skal pålegges hel eller delvis lagringsplikt kan det blant annet tas hensyn til antallet av sluttbrukere knyttet til det elektroniske kommunikasjonsnett- eller tjeneste, om tilgangen ytes mot vederlag og tilbyders økonomiske forhold. Beskrivelsen er ikke uttømmende.

Til ekomloven § 2-9 tredje ledd

Bestemmelsen første punktum om utlevering av identifikasjonsopplysninger til politi og påtalemyndighet er uavhengig av taushetsplikten videreføres uendret. Det samme gjelder bestemmelsens andre punktum om vitnemål for retten. Tredje punktum endres med den følge at det bare er identifikasjonsdata nevnt i tredje ledd første punktum som uavhengig av taushetsplikten i § 2-9 første ledd kan utleveres til andre myndigheter i medhold av lov.

Til ekomloven § 2-9 nytt femte ledd

Bestemmelsen gjelder påtalemyndigheten og politiets tilgang til data som er lagret enten for å legge til rette for etterforskning og rettsforfølgning av alvorlig kriminalitet etter § 2-8 andre ledd eller for tilbydernes forretningsdrift, jf. § 2-7 andre ledd. Taushetsplikten etter § 2-9 første ledd er ikke til hinder for at data som er lagret til disse formålene utlevers til påtalemyndighet og politi når retten har gitt tillatelse etter reglene i straffeprosessloven. Innhenting av dataene i disse tilfelle forutsetter derfor ikke at tilbyder er fritatt fra taushetsplikten når det foreligger et utleveringspålegg fra retten. Det understrekes at det i fremtiden ikke skal være adgang til å hente ut lagrede data som ledd i vitneforklaring etter straffeprosessloven § 230, jf, § 118.

Påtalemyndighetens og politiets tilgang til identifikasjonsdata som er omfattet av § 2-9 tredje jf. fjerde ledd, berøres ikke av unntaket i femte ledd.

8. FORSLAG TIL ENDRING I LOV OM ELEKTRONISK KOMMUNIKASJON

Ekomloven § 2-7 annet ledd kan lyde:

Trafikkdata, *lokaliseringsdata og data nødvendig for å identifisere abonnenten eller brukeren* skal slettes eller anonymiseres så snart de ikke lenger er nødvendig til kommunikasjons- eller faktureringsformål *eller for å oppfylle lagringsplikten i § 2-8 første ledd,* med mindre annet er bestemt i eller i medhold av lov. Annen behandling av *slike data* krever samtykke fra bruker.

Ekomloven § 2-8 nytt annet ledd kan lyde:

Tilbyder som nevnt i første ledd skal lagre trafikkdata, lokaliseringsdata og data nødvendig for å identifisere abonnenten eller brukeren i X måneder for å legge til rette for etterforskning og rettsforfølgning av alvorlige straffbare forhold. Plikten etter første punktum gjelder data som genereres eller behandles i tilbyders elektroniske kommunikasjonsnett ved bruk av fasttelefoni, mobiltelefoni, internettelefoni, internettaksess og e-post.

Ekomloven § 2-8 nåværende tredje ledd blir fjerde ledd og kan lyde:

Myndigheten kan gi forskrifter om tilretteleggingsplikten etter første ledd. *Myndigheten kan for å sikre oppfyllelse av plikten til å lagre data etter andre ledd gi forskrift, treffe enkeltvedtak eller inngå avtale om tilbyders gjennomføring av tiltak i henhold til andre ledd. Myndigheten kan i særlige tilfelle ved forskrift eller enkeltvedtak helt eller delvis frita fra plikten til å lagre data. Myndigheten kan helt eller delvis pålegge andre enn de som omfattes av andre ledd plikt til å lagre data dersom dette må til for å oppnå formålet med bestemmelsen.*

Ekomloven § 2-9 tredje ledd kan lyde:

Taushetsplikten er ikke til hinder for at det gis opplysninger til påtalemyndigheten eller politiet om avtalebasert hemmelig telefonnummer eller andre abonnementsopplysninger, samt elektronisk kommunikasjonsadresse. Det samme gjelder ved vitnemål for retten. Taushetsplikten er heller ikke til hinder for at opplysninger som nevnt i første *punktum* gis til annen myndighet i medhold av lov.

Ekomloven § 2-9 nytt femte ledd kan lyde:

Taushetsplikten er heller ikke til hinder for at andre data enn de som er nevnt i tredje ledd kan utleveres til påtalemyndigheten eller politiet etter rettens kjennelse i medhold av straffeprosesslovens bestemmelser om beslag og utleveringspålegg.

Ekomloven § 2-9 nåværende femte ledd blir sjette ledd.

Ekomloven § 2-9 nåværende sjette ledd blir syvende ledd.

9. FORSLAG TIL ENDRING I STRAFFEPROSESSLOVEN

Straffeprosessloven § 210 første ledd kan lyde:

§ 210. Ting som antas å ha betydning som bevis, kan retten pålegge besitteren å utlevere såfremt han plikter å vitne i saken. *Retten kan likevel bare pålegge besitteren å utlevere data som er lagringspliktige etter ekomloven 2-8 annet ledd såfremt noen med skjellig grunn mistenkes for en handling eller forsøk på en handling som etter loven kan medføre straff av fengsel i 3 år eller mer, eller som rammes av straffeloven §§ 91, 91a, 104 a, 132 b, 145 annet ledd, 145 a, 162, 201a, , 203, 204a, 317, jf. §§ 162 eller 390 a.* Reglene i § 137 og domstolsloven § 206 gjelder tilsvarende.

10. FORSLAG TIL ENDRING I EKOMFORSKRIFTEN

§ 7-2 første ledd kan lyde:

"*Tilbyder skal bevare taushet om andre lokaliseringsdata enn trafikkdata etter ekomloven § 2-9 og skal slette eller anonymisere slike lokaliseringsdata etter ekomloven § 2-7 annet ledd. Annen behandling av lokaliseringsdata enn den som følger av lagringsplikten i ekomloven § 2-8 annet ledd kan bare skje i anonymisert form.* Med lokaliseringsdata menes data som behandles i et elektronisk kommunikasjonsnett og som angir den geografiske plassering av terminalutstyret som brukeren av offentlig kommunikasjonstjeneste anvender".