DET KONGELIGE
JUSTIS- OG POLITIDEPARTEMENT

Prop. 49 L

(2010–2011)

Proposisjon til Stortinget (forslag til lovvedtak)

Endringer i ekomloven og straffeprosessloven mv. (gjennomføring av EUs datalagringsdirektiv i norsk rett)

Innhold

1 Innledning og sammendrag 7
1.1 Innledning 7
1.1.1 Om høringen 8
1.2 Hovedpunkter i lovforslaget 8

2 Om direktivet 11
2.1 Bakgrunnen for direktivet 11
2.2 Kort om direktivet 11
2.3 Nærmere om nasjonal prosess og høring 12

3 Forholdet til menneskerettighetene 14
3.1 Innledning 14
3.2 Gjeldende rett, høringsnotatets forslag og høringsinstansenes syn 14
3.2.1 Retten til privatliv (EMK artikkel 8) 14
3.2.2 Ytringsfrihet, herunder pressens kildevern og forsamlings- og foreningsfriheten 19
3.2.3 Uskyldspresumsjonen 22
3.2.4 Øvrige forpliktelser 23
3.3 Departementets vurderinger 24
3.3.1 Innledning 24
3.3.2 Retten til privatliv (EMK artikkel 8) 24
3.3.3 Ytringsfrihet, herunder pressens kildevern og forsamlings- og foreningsfriheten 28
3.3.4 Uskyldspresumsjonen 30
3.3.5 Øvrige forpliktelser 31

4 Implementering av datalagrings-direktivet i Europa 32
4.1 Danmark 32
4.2 Finland 33
4.3 Sverige 33
4.4 Andre EU-land 35

5 Behovet for data i kriminalitets-bekjempelsen 36
5.1 Innledning 36
5.2 Høringsnotatets forslag 37
5.3 Høringsinstansenes syn 37
5.3.1 Høringsinstansene – generelt om behovet for datalagringsdirektivet 37
5.3.2 Høringsinstansene om internasjonale forpliktelser og internasjonalt politi- og påtalesamarbeid 39
5.3.3 Høringsinstansene om alternativer til bruk av historiske data 39
5.3.4 Høringsinstansene om omgåelse av datalagringsdirektivet 39
5.3.5 Høringsinstansene om behovet for data og ulike typer datas betydning 40
5.3.6 Høringsinstansene om saksområder og sakseksempler 41
5.4 Tematisk sammenstilling av områder behandlet i høringsuttalelsene 41
5.4.1 Innledning 41
5.4.2 Nærmere om offentlige utredninger m.v. 41
5.4.3 Nærmere om internasjonale forpliktelser og internasjonalt politi- og påtalesamarbeid 42
5.4.4 Nærmere om alternativer til bruk av historiske data 43
5.4.5 Nærmere om omgåelse av datalagringsdirektivet 44
5.4.6 Nærmere om behovet for data og ulike typer datas betydning 45
5.4.7 Nærmere om saksområder med konkrete sakseksempler 53
5.5 Departementets vurdering 60
5.5.1 Internasjonale forpliktelser og internasjonalt politi- og påtalesamarbeid 60
5.5.2 Alternativer til bruk av historiske data 60
5.5.3 Omgåelse av datalagringsdirektivet 60
5.5.4 Behovet for data og ulike typer datas betydning 61
5.5.5 Saksområder med konkrete sakseksempler 62

6 Personvern 64
6.1 Innledning 64
6.2 Høringsnotatets redegjørelse 64
6.3 Høringsinstansenes syn 65
6.4 Departementets vurdering 68

7 Hvem skal lagre 71
7.1 Gjeldende rett 71
7.2 Høringsnotatets forslag 71
7.3 Høringsinstansens syn 71
7.4 Departementets vurdering 72
7.5 Nærmere om lovforslaget 72

8 Hva skal lagres ... 73
8.1 Gjeldende rett ... 73
8.2 Høringsnotatets forslag ... 73
8.3 Høringsinstansenes syn ... 74
8.4 Departementets vurdering ... 75
8.4.1 Om lagring og bredbåndstelefoni 75
8.4.2 Om tilgjengelighet til data i nett og systemer ... 76
8.4.3 Om mislykkede oppringninger og tapte anrop ... 76
8.4.4 Om kvaliteten på de lagrede data.. 77
8.5 Nærmere om lovforslaget ... 77

9 Lagringstid ... 79
9.1 Gjeldende rett ... 79
9.2 Høringsnotatets forslag ... 79
9.3 Høringsinstansenes syn ... 80
9.4 Departementets vurdering ... 81
9.5 Nærmere om lovforslaget ... 82

10 Konkurransen innenfor elektronisk kommunikasjon ... 83
10.1 Innledning ... 83
10.2 Høringsinstansenes syn ... 83
10.3 Departementets vurdering ... 84

11 Lagringssted og informasjonssikkerhet ... 86
11.1 Gjeldende rett ... 86
11.2 Høringsnotatets forslag ... 86
11.3 Høringsinstansenes syn ... 86
11.4 Departementets vurdering ... 87
11.4.1 Informasjonssikkerhet ... 87
11.4.2 Lagringssted ... 91

12 Utlevering av data i etterforskningsøyemed ... 92
12.1 Gjeldende rett om politiets hjemler for innhenting av elektronisk lagrede data ... 92
12.2 Metodekontrollutvalgets forslag i NOU 2009: 15 ... 94
12.3 Datalagringsdirektivets betydning for reguleringen av tilgangen til lagrede data ... 95
12.4 Høringsnotatets forslag ... 95
12.5 Høringsinstansenes syn ... 96
12.5.1 Vilkårene for utlevering av data ... 96
12.5.2 Kravet om mistanke til en bestemt person ... 97
12.5.3 Kravet om tre års strafferamme ... 99
12.5.4 Domstolskontroll med utlevering av data ... 102
12.6 Departementets vurdering ... 103

13 Utlevering av data i avvergende og forebyggende øyemed ... 108
13.1 Gjeldende rett ... 108
13.2 Høringsnotatet og høringsinstansenes syn ... 108
13.3 Departementets vurdering ... 108
13.4 Straff for brudd på tilbyders taushetsplikt ved utlevering i forebyggende øyemed ... 109

14 Regler for tilgang til data for andre ... 111
14.1 Innledning ... 111
14.2 Gjeldende rett ... 111
14.2.1 Om andre myndigheters tilgang ... 111
14.2.2 Om utlevering av lagrede data som bevis i sivile saker ... 112
14.3 Høringsnotatets forslag ... 113
14.4 Høringsinstansenes syn ... 113
14.4.1 Om andre myndigheters tilgang ... 113
14.4.2 Om utlevering av lagrede data som bevis i sivile saker ... 114
14.5 Departementets vurdering ... 115
14.5.1 Om andre myndigheters tilgang ... 115
14.5.2 Særlig om Finanstilsynets tilgang ... 117
14.5.3 Om bruk av trafikkdata som bevis i sivile saker ... 119

15 Tilsyn ... 120
15.1 Gjeldende rett ... 120
15.2 Høringsnotatets forslag ... 120
15.3 Høringsinstansenes syn ... 121
15.4 Departementets vurdering ... 122
15.5 Nærmere om lovforslaget ... 123
15.5.1 Statistikk ... 123

16 Økonomiske og administrative konsekvenser ... 124
16.1 Gjeldende rett ... 124
16.2 Høringsnotatets forslag ... 124
16.3 Økonomiske utredninger og analyser ... 124
16.4 Høringsinstansenes syn ... 125
16.5 Departementets vurdering ... 128
16.5.1 Nærmere om konsekvensene for myndighetene ... 128
16.5.2 Nærmere om konsekvensene for tilbydere av ekomnett og -tjenester ... 129
16.5.3 Nærmere om konsekvensene for domstolene ... 130
16.6 Oppsummert om administrative og økonomiske konsekvenser ... 130

17 Merknader til de enkelte bestemmelsene i lovforslaget ... 131
17.1 Merknader til endringer i straffeprosessloven 131
17.2 Merknader til endring i politiloven 133
17.3 Merknader til endringer i ekomloven 133
17.4 Merknader til endring i tvisteloven 136
17.5 Merknader til endring i verdipapirhandelloven 136
17.6 Merknader til ikrafttredelses-bestemmelsen 136

Forslag til lov om endringer i ekomloven og straffeprosessloven mv. (gjennomføring av EUs datalagringsdirektiv i norsk rett) 138

DET KONGELIGE
JUSTIS- OG POLITIDEPARTEMENT

Prop. 49 L

(2010–2011)

Proposisjon til Stortinget (forslag til lovvedtak)

Endringer i ekomloven og straffeprosessloven mv. (gjennomføring av EUs datalagringsdirektiv i norsk rett)

Tilrådning fra Justis- og politidepartementet av 10. desember 2010, godkjent i statsråd samme dag.
(Regjeringen Stoltenberg II)

1 Innledning og sammendrag

1.1 Innledning

Justisdepartementet legger i denne proposisjonen frem et forslag til hvordan EUs direktiv 2006/24/EF om lagring av data fremkommet ved bruk av offentlig elektronisk kommunikasjonstjeneste og offentlig elektronisk kommunikasjonsnett med endring av direktiv 2002/58/EC (datalagringsdirektivet) kan gjennomføres i norsk rett. Det fremmes forslag til endringer i lov om elektronisk kommunikasjon, straffeprosessloven, politiloven, tvisteloven og verdipapirhandelloven.

Formålet med datalagringsdirektivet 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 straffeforfølge alvorlig kriminalitet.

Ved bruk av elektronisk kommunikasjon genereres ulike typer data. Bruker- og abonnementsdata er de mest opplagte, men også lokasjonsdata og trafikkdata produseres. Disse dataene kan si noe om hvem som har kommunisert med hvem, hvor kommunikasjonen har funnet sted, når og hvordan. I etterforskning, oppklaring og straffeforfølging av kriminalitet er denne type data nyttige og viktige. Departementets mål med lovforslagene er å legge til rette for at politi og påtalemyndighet skal kunne få utnytte det virkemidlet som data representerer. I dag lagrer tilbydere av offentlig elektronisk kommunikasjonstjeneste eller offentlig elektronisk kommunikasjonsnett i Norge data for egne kommunikasjons- og faktureringsformål. Trafikkdata er nødvendige for overføring av kommunikasjon i et elektronisk kommunikasjonsnett eller for fakturering av slik overføring. Politiet har i dag mulighet til å få tilgang til disse dataene for å etterforske eller forebygge straffbare handlinger. Finanstilsynet har også hjemler for tilgang til data som er nødvendige for at tilsynet skal kunne utføre sin virksomhet. Denne tilgangen videreføres av hensyn til underliggende internasjonale forpliktelser.

Det prinsipielt nye med gjennomføringen av datalagringsdirektivet er at tilbyderne pålegges en plikt til å lagre, at flere data enn i dag skal lagres, at lagringstiden vil bli lengre og at lagring

skal foregå for et annet formål enn tilbyders eget, nemlig kriminalitetsbekjempelse.

1.1.1 Om høringen

Forslaget om å gjennomføre datalagringsdirektivet i norsk rett har gitt grunnlag for et stort engasjement og skapt betydelig debatt i det norske samfunnet på tvers av tradisjonelle politiske skillelinjer.

Samferdselsdepartementet, Justisdepartementet og Fornyingsdepartementet sendte 8. januar 2010 på høring et forslag til hvordan datalagringsdirektivet kan gjennomføres i norsk rett. Høringsfristen var 12. april 2010. Bidragene i den offentlige høringsrunden har vært mange. Over 130 skriftlige innspill kom inn, i tillegg til flere innlegg på Samferdselsdepartementets blogg. Det ble også arrangert høringsmøter om saken.

Følgende høringsinstanser har eksplisitt gitt uttrykk *for* at de mener datalagringsdirektivet må gjennomføres i norsk rett: Politidirektoratet, Kripos, Økokrim, Det nasjonale statsadvokatembetet, Riksadvokaten, Politiets sikkerhetstjeneste, Politijuristene, Norsk Narkotikapolitiforening, Norges politilederlag, Politiets Fellesforbund, Stine Sofies Stiftelse, Næringslivets sikkerhetsråd, Hovedorganisasjonen for universitets- og høyskoleutdannede, HSH, NHO, TEKNA og Finansnæringens fellesorganisasjon.

Følgende høringsinstanser har gitt eksplisitt uttrykk for at de mener datalagringsdirektivet *ikke* må gjennomføres i norsk rett: Datatilsynet, Universitetet i Oslo – matematisk naturvitenskapelige fakultet, Telenor, NetCom, Tele2, Ventelo, Altibox, NRK, Advokatforeningen, Norsk Juristforbund – privat, KROM, Elektronisk forpost Norge, Forsvarergruppen av 1977, Elektronikkbransjen, EL og IT forbundet, Folkets høringsuttalelse, Redd Barna, Abelia, IKT-Norge, YS, Fagforbundet avdeling Lillehammer, Foreningen Fritt Norden, Nardo Nidarvoll Arbeiderlag, Norwegian Unix User Group, Norsk Presseforbund, FriBit, Norsk journalistlag, ICJ-Norge, NITO, Norsk PEN, Norsk redaktørforening, Norsk presseforbund, Forbrukerrådet, LO, Stopp DLD, Samfunnsorganisasjonen Demos, LO-Trondheim, Troms Nei til EU, Akershus, Aust Agder, Hordaland, Rogaland, Sogn og fjordane, Telemark, Vestfold og Østfold, Hordaland senterungdom, Oppland senterparti, Norsk Målungdom, Levanger Venstre, Nord-Trøndelag Venstre, Raudt/Rødt Høyanger, Sogn og fjordane, Sør-Trøndelag og Senterungdommen. I tillegg har enkelte privatpersoner uttrykt sin motstand mot direktivet. Øvrige høringsinstanser har ikke tatt stilling til for eller mot, men har likevel kommentert de ulike forslagene i høringsnotatet.

Flere av høringsinstansene blant annet IKT-Norge, Abelia og Europabevegelsen har gitt uttrykk for at norske myndigheter bør avvente EUs evaluering av datalagringsdirektivet før man gjennomfører det i norsk rett.

En av hovedinnvendingene mot datalagringsdirektivet er spørsmålet om direktivet er i tråd med den europeiske menneskerettighetskonvensjonen (EMK). Denne problemstillingen drøftes nærmere i kapittel 3.

Politiet har gitt uttrykk for at datalagringsdirektivet er helt nødvendig for å kunne bekjempe alvorlig kriminalitet. Det har imidlertid av mange høringsinstanser blitt stilt spørsmål ved dette, og om det er egnet for å nå dette målet. Departementet har derfor sett det som nødvendig å vie stor plass i proposisjonen til å dokumentere behovet for data i kriminalitetsbekjempelsen, jf. kapittel 5.

Mange høringsinstanser påpeker at det er betydelige personvernutfordringer knyttet til lagring av store mengder kommunikasjonsdata for hele befolkningen. Departementet er langt på vei enig i dette, og er derfor opptatt av å ivareta borgernes krav på kommunikasjons- og integritetsvern på best mulig måte. Spørsmål om personvern behandles i kapittel 6. Ekombransjen har påpekt at en lagringsplikt vil kunne påvirke konkurransen innenfor markedet for elektronisk kommunikasjon i den forstand at det vil kunne bli skjevheter til tross for at formålet med direktivet er å harmonisere. Spørsmål om konkurransen innenfor elektronisk kommunikasjon er behandlet blant annet i kapittel 8 og 10.

1.2 Hovedpunkter i lovforslaget

Høringsuttalelsene har gitt nyttig informasjon for arbeidet med lovforslaget. Det foreliggende lovforslaget har som siktemål å belyse og imøtekomme politiets behov slik det kom frem i høringen. Samtidig er hensynet til personvernet søkt ivaretatt blant annet ved at det foreslås strengere regler for politiets tilgang til data.

Lovforslaget innfører en lagringsplikt for tilbydere av offentlig ekomnett og -tjenester, samtidig som det stilles strenge krav til informasjonssikkerhet og sletting. Det er videre foreslått innskjerpelser sammenlignet med dagens regler om utlevering av data til politi og påtalemyndighet. Også for Finanstilsynet er det foreslått innskjerpelser ved at det innføres domstolskontroll ved utleve-

ring av data. Det foreslås ingen endringer i reglene om Politiets sikkerhetstjenestes tilgang til data.

Hvem skal lagre data

Det fremgår av datalagringsdirektivets artikkel 1 at det er tilbyder av offentlig elektronisk kommunikasjonstjeneste eller offentlig elektronisk kommunikasjonsnett som skal lagre. Departementet foreslår at det er ekomlovens definisjon av tilbydere av ekomnett og -tjenester som skal legges til grunn for hvem som skal lagre. 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 8.5.

Hva skal lagres

Det fremgår av datalagringsdirektivets artikkel 5 hvilke kategorier av data som skal lagres. Departementets forslag til lovendring vil medføre innføring av lagringsplikt for trafikkdata, lokaliseringsdata og abonnements/brukerdata som fremkommer ved bruk av elektronisk kommunikasjon som fasttelefoni, mobiltelefoni, internettaksess, e-post og bredbåndstelefoni.

Lagringstid

Departementet foreslår at det innføres en lagringsplikt for data lagret i henhold til datalagringsdirektivet på 12 måneder.

Lagringssted og informasjonssikkerhet

Departementet går inn for at det skal være opp til den enkelte tilbyder å velge lagringsløsning. Departementet har særlig vektlagt personvernmessige hensyn når det ikke foreslås å etablere en sentral lagringsløsning. Dette utelukker imidlertid ikke at små tilbydere kan gå sammen om en felles lagringsløsning. I tillegg til de personvernmessige vurderingene, har departementet også vurdert kostnader samt sikkerhetsmessige og konkurransemessige aspekter. Departementet mener informasjonssikkerheten kan ivaretas på en tilfredsstillende måte ved lokal lagring.

Regler for tilsyn

Det foreslås at dagens tilsynsordning, med et delt tilsynsansvar mellom Post- og teletilsynet og Datatilsynet, videreføres. Departementet vil følge opp arbeidet med en styrking av den samarbeidsavtalen som allerede foreligger mellom de to tilsynene.

Regler for tilgang

Politiets behov for data er utgangspunktet for utformingen av reglene. Abonnementsopplysninger, herunder også elektronisk kommunikasjonsadresse er mindre beskyttelsesverdige opplysninger. Disse bør derfor fortsatt være underlagt taushetsplikt jf. ekomloven § 2-9 tredje ledd der utlevering ikke forutsetter kjennelse fra retten.

Forslaget innebærer at data bare skal utleveres etter rettens kjennelse i saker der det foreligger skjellig grunn til mistanke om en straffbar handling som kan medføre fengsel i 4 år eller mer. Basestasjonssøk er mest inngripende i forhold til personvernet, blant annet fordi man da får med seg mye overskuddsinformasjon. Utlevering av data etter basestasjonssøk forutsetter rettens kjennelse og at den straffbare handlingen kan medføre straff av fengsel i 5 år eller mer. I begge tilfeller skal utlevering av data dessuten kunne skje dersom handlingen er utøvet som ledd i organisert kriminalitet og kan straffes med fengsel i 3 år eller mer. Det åpnes også for utlevering i enkelte andre typer saker som vil være særlig vanskelig å etterforske uten tilgang til data (uttømmende oppregning av straffebud). I tillegg kreves det at data skal ha vesentlig betydning for etterforskningen og at utlevering for øvrig er nødvendig og forholdsmessig, jf. straffeprosessloven § 170 a.

En sentral rettssikkerhetsgaranti i forbindelse med utformingen av utleveringsbestemmelsen er at det heretter ikke skal utleveres data uten etter kjennelse fra retten. Mistenkte skal underrettes om dette med mindre retten beslutter utsatt underretning. I så fall skal det straks oppnevnes offentlig advokat for mistenkte, jf. straffeprosessloven § 100 a. Hensikten med advokaten er å sikre kontradiksjon og samtidig påse at vilkårene for utleveringspålegg er oppfylt.

Økonomiske og administrative konsekvenser

Departementet foreslår ingen lovendringer knyttet til kostnader ved innføring av datalagringsdirektivet. Dagens bestemmelser om kostnader knyttet til tilrettelegging for lovbestemt tilgang opprettholdes. Det er ikke tatt stilling til hvem som skal dekke kostnader tilknyttet lagringsplikten. En modell for beregning og fordeling mellom ekomtilbyderne og justismyndighetene vil bli utarbeidet.

Det foreslås at Post- og teletilsynets eventuelle økte kostnader dekkes gjennom en kostnadsriktig justering av tilsynets gebyrer. Datatilsynets og domstolenes økte kostnader foreslås dekket innenfor gjeldende budsjettrammer. Behov for styrking av budsjettet må eventuelt vurderes i samband med de årlige budsjettproposisjonene.

2 Om direktivet

2.1 Bakgrunnen for direktivet

EU vedtok i 2004 en deklarasjon om bekjempelse av terror (Declaration on Combating Terrorism). Bakgrunnen for denne deklarasjonen var blant annet terrorangrepene i Madrid i mars 2004. I deklarasjonen er behovet for felles virkemidler for å bekjempe terror understreket, og Rådet blir blant annet bedt om å komme med forslag til etablering av felles regler for lagring av data fremkommet ved bruk av elektronisk kommunikasjon. Et forslag til rådsbeslutning om datalagring ble fremmet av Sverige, Storbritannia, Frankrike og Irland i april 2004. Rådsforslaget ble avvist av EU-parlamentet i september 2005 blant annet på grunn av at forslaget var fundert i artikkel 31 og 34 i EU-traktaten, under den såkalte «tredje søyle» som handler om samarbeid på justis- og innenriksområdet. EU-kommisjonen fremmet i september 2005 et forslag til direktiv med den begrunnelse at de mente regler for datalagring hører hjemme i det indre marked. Forslaget fra Kommisjonen ble etter forhandlinger med EU-parlamentet og Rådet endret på enkelte områder, og endelig vedtatt i mars 2006.

2.2 Kort om 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 straffeforfølge alvorlig kriminalitet. Fristen for implementering av direktivet var 15. september 2007 med en utsettelse til 15. mars 2009 for data knyttet til Internett.

Direktivet legger klare føringer for hvem som skal lagre og hva som skal lagres. Det skal lagres en mengde data som er nødvendig for å spore og identifisere kilder til en kommunikasjon, dato, tid, sted og varighet. Også data som sier noe om type kommunikasjon, hvilket utstyr som benyttes og lokalisering skal lagres. Innhold i kommunikasjonen skal ikke lagres. 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 tilgjengelige. Tilbyderne skal ikke etablere systemer for å kunne lagre data som de ikke har tilgjengelig ved produksjon av tjenester per i dag. Direktivet inneholder også visse krav til informasjonssikkerhet hos tilbyder.

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. Denne evalueringen er forsinket og det er ikke kjent hva konklusjonene i rapporten vil bli.

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 utarbeidet flere dokumenter som skal gi veiledning i hvordan medlemslandene skal tolke og tilnærme seg pliktene i direktivet. Dokumentene er såkalte «position papers», og ikke alle er ferdigstilte. Eksempler på «position papers» som er ferdigstilt er dokumenter om web-mail, spam e-post, transittilbydere og forståelsen av termen «Internet Telephony». Departementet har gjennom EFTA-sekretariatet fulgt arbeidet i ekspertgruppen og har hatt nytte av drøftingene i gruppen ved utarbeidelsen av lovforslaget.

2.3 Nærmere om nasjonal prosess og høring

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 hvordan artikkel 5 i direktivet om hva som skal lagres skal forstås, 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 notatet som ble sent på høring i januar 2010. 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.

Også andre aktører enn departementet har utredet spørsmål knyttet til eventuell innføring av datalagringsdirektivet i norsk rett. Personvernkommisjonen avga sin utredning NOU 2009:1 Individ og integritet i januar 2009. Innstillingen er å finne på *www.regjeringen.no/fad.* Om datalagringsdirektivet uttaler personvernkommisjonen (vedlegg 1 på side 221):

> «Vi kan ikke støtte innføring av direktivet uten at behovet for utvidet lagring er bedre dokumentert. Både politiets og andre nasjonale myndigheters behov for utvidet lagring og tilgang til trafikkdata i det omfang som er foreslått må derfor begrunnes bedre.
>
> Direktivets overordnede formål er å bekjempe alvorlig kriminalitet. Den teknologiske utvikling har forandret metodene som brukes både ved terror og andre former for kriminalitet. Dette har skapt et behov for nye metoder ved etterforskning og bekjempelse av kriminalitet. I fotsporene til den teknologiske utviklingen følger kriminelle som søker å utnytte denne til terrorisme og andre forbrytelser. Derfor er det viktig for politi og påtalemyndigheter å ha tilgang til de verktøyene man til en hver tid trenger til bekjempelse av kriminalitet. Det er også viktig at dette skjer innenfor demokratiske og klare rammer. Vi utelukker ikke at trafikkdata kan være viktige for politiet ved etterforskning og oppklaring av kriminelle handlinger, men vi stiller oss likevel kritisk til beslutningsgrunnlaget for den omfattende lagringsplikten som følger av direktivet. Derfor etterlyser kommisjonen dokumentasjon av politiets og andre myndigheters behov for trafikkdata i det omfang som følger av direktivet.
>
> Personvernkommisjonen ser behovet for et regelverk både for lagring og utlevering av trafikkdata. I dag får politiet tilgang til trafikkdata fordi teletilbydere lagrer opplysningene for kommunikasjons- og faktureringsformål. Politiets tilgang til opplysninger er regulert i ulike regler og gjennom praksis fra Post- og teletilsynet. Regelverket er uoversiktlig og vanskelig tilgjengelig for borgerne. Dette er i seg selv en svakhet. Videre ser man nå en utvikling i teleoperatørenes faktureringsrutiner som kan føre til at politiet mister denne tilgangen til trafikkdata som de til nå har hatt. Som en følge av den teknologiske utviklingen går teletilbyderne fra å fakturere for bruk (som fordrer lagring av trafikkdata) til å fakturere for tilgang. Dermed har de ikke behov for å lagre trafikkdata. En slik utvikling gjør at politiet vil miste verdifull informasjon. Etter Personvernkommisjonens oppfatning er det derfor ønskelig med en grundig utredning av behovet for et regelverk som sikrer politiets arbeidsmetoder og ivaretar personvernet.«

I Metodekontrollutvalgets utredning NOU 2009: 15 «Skjult informasjon – åpen kontroll» omtales datalagringsdirektivet. Dette gjøres imidlertid kort idet utvalget avgrenser sitt mandat mot direktivet (utredningen kapittel 20.4 på side 219):

> «I dag lagres trafikkdata hos norske teletilbydere i inntil tre til fem måneder av faktureringshensyn. Dette er fastsatt i konsesjonsvilkår fra Datatilsynet. Som trafikkdata regner direktivet data som er nødvendig for å spore og identifisere kilden til kommunikasjon, data som er nødvendig for å fastslå kommunikasjonens bestemmelsessted og data som er nødvendig for å lokalisere mobilt utstyr, jf. direktivet artikkel 5. En del av disse dataene lagres ikke nødvendigvis hos norske teletilbydere i dag. Datalagringsdirektivet sier imidlertid ikke noe om hvilke vilkår som skal gjelde for politiets tilgang til trafikkdata, og berører dermed ikke utvalgets vurderinger direkte.»

Samtidig har utvalget drøftet regler for politiets tilgang til data, jf. nærmere omtale under kapittel 12.2. Utredningen finnes i sin helhet på *www.regjeringen.no/jd*.

Samferdselsdepartementet, Justisdepartementet og Fornyingsdepartementet sendte 8. januar 2010 ut et felles høringsnotat med forslag til hvordan datalagringsdirektivet eventuelt kan gjennomføres i norsk rett. Høringsfristen var 12. april 2010. Det kom inn over 130 høringssvar, samt en rekke innlegg på bloggen som ble opprettet i tilknytning til høringen.

3 Forholdet til menneskerettighetene

3.1 Innledning

Flere menneskerettskonvensjoner kan tenkes å ha betydning for om og hvordan datalagringsdirektivet bør gjennomføres i norsk rett. Både Europarådets konvensjon 4. november 1950 om beskyttelse av menneskerettighetene og de grunnleggende friheter (EMK), FNs konvensjon 16. desember 1966 om sivile og politiske rettigheter (SP) samt FNs konvensjon 20. november 1989 om barns rettigheter (FNs barnekonvensjon) gjelder som en del av norsk rett, jf. lov 21. mai 1999 nr. 30 om styrking av menneskerettighetenes stilling i norsk rett (menneskerettsloven). Av menneskerettsloven § 3 følger at konvensjonene ved motstrid skal gå foran bestemmelser i annen norsk lovgivning.

3.2 Gjeldende rett, høringsnotatets forslag og høringsinstansenes syn

3.2.1 Retten til privatliv (EMK artikkel 8)

EMK artikkel 8 om retten til respekt for privatliv og familieliv 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.»

I *høringsnotatet* kapittel 4.2 ble det gjort nærmere rede for forholdet til EMK artikkel 8. Departementenes utgangspunkt var at datalagringsdirektivets krav til lagring og utlevering innebar et inngrep i retten til privatliv, herunder korrespondanse.

EMK artikkel 8 nr. 2 åpner imidlertid for at slike inngrep kan rettferdiggjøres dersom inngrepet har hjemmel i lov, ivaretar nærmere angitte formål og er nødvendig i et demokratisk samfunn for å oppfylle ett eller flere legitime formål. Lovkravet ble foreslått oppfylt ved forslaget til endring i ekomloven § 2-8 nytt annet ledd om lagringsplikt. Om direktivets formål og nødvendighet ble det redegjort slik:

> «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 la departementene til grunn at plikten til å lagre data som nedfelt i datalagringsdirektivet, ikke var i strid med EMK artikkel 8. Det ble også vist til at dette var i samsvar med den konklusjonen EU hadde 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.»

En rekke *høringsinstanser* uttalte seg på dette punktet. *Riksadvokaten*, *Det nasjonale statsadvokatembetet*, *Hordaland statsadvokatembeter*, *Oslo statsadvokatembeter*, *Kripos* og *ØKOKRIM* mener at den foreslåtte gjennomføringen av direktivet ikke vil være i strid med EMK artikkel 8.

De fleste av disse høringsinstansene anerkjenner at gjennomføringen av direktivet vil medføre et inngrep etter EMK artikkel 8 nr. 1. Det kan likevel rettferdiggjøres etter EMK artikkel 8 nr. 2. Det vises særlig til at lagring av data er viktig for å etterforske, oppklare og rettsforfølge en rekke kriminalitetstyper, og at manglende innføring av direktivet kan svekke myndighetenes muligheter til å vareta borgernes trygghet, frihet og oppklare alvorlig kriminalitet. Lagringen vil også kunne være nødvendig for å vareta andres rettigheter, herunder rettighetene til kriminalitetsofre. I den forbindelse trekkes avgjørelsen fra Den europeiske menneskerettsdomstol (EMD) i saken *K.U. mot Finland*, 2. desember 2008 (nr. 2872/02) frem. Det hevdes at avgjørelsen kan tas til inntekt for at statene er forpliktet til å sørge for at data lagres. Det vises blant annet til at bare slik kan andre legitime rettigheter, herunder personvernhensyn og fundamentale rettigheter til en rekke kriminalitetsofre, gis et effektivt vern. Om betydningen av data for å ivareta den enkelte borgers personvern skriver *Kripos* i sin høringsuttalelse:

> «Når det stilles spørsmål om direktivet er forenlig med artikkel 8, tas det utgangspunkt i personvernet til de som berøres av direktivet, nemlig brukerne av elektroniske kommunikasjonsmidler. En annen innfallsvinkel er å spørre om direktivet er en forutsetning for at Norge skal ivareta sine forpliktelser etter artikkel 8, og da med utgangspunkt i personvernet til ofrene for kriminelle handlinger. […] Kripos er også av den oppfatning at direktivet er nødvendig for at Norge skal verne privatlivet til den enkelte borger, slik EMK artikkel 8 foreskriver. En viser for øvrig til EMDs avgjørelse i saken K.U. mot Finland […] I domspremissene legges det til grunn at myndighetene har en positiv forpliktelse til å sørge for mekanismer som gjør det mulig å identifisere og straffeforfølge personer som krenker andres liv, helbred og retten til privatliv. Uten en implementering av datalagringsdirektivet kan det bli vanskelig å ivareta denne forpliktelsen.»

Mange av instansene viser også generelt til samfunnsinteressen (alle borgernes interesse) i at alvorlig kriminalitet som svekker samfunnsinstitusjonene (alvorlig organisert kriminalitet, terror, korrupsjon, motarbeidelse av rettsvesenet m.v.) oppklares. Om lagringspliktens betydning for personvernet uttaler ØKOKRIM at:

> «[…] lagring av trafikkdata innenfor de rammer datalagringsdirektivet oppstiller, vil utgjøre en relativt liten andel av den samlede mengden personlige data som lagres i dag. I tillegg til personregistre, kunderegistre, pasientregistre og informasjon som lagres hos finansinstitusjoner, legger et flertall av oss igjen en overveldende mengde elektroniske spor som ledd i våre hverdagslige gjøremål, slik som ved bruk av bankkort, betaling i bomring, bruk av kollektivtrafikk og på jobben.
>
> Den overveldende mengden av elektroniske spor og personlige opplysninger vi hver dag frivillig legger igjen etter oss, kan etter vårt syn tyde på at befolkningen ikke anser slike data som så veldig personlige eller sensitive. Det er dermed ikke nødvendigvis slik at lagring av trafikkdata vil virke særlig hemmende på folks personlige utfoldelse og frimodighet.
>
> Det er videre av stor betydning for vurderingen av lagringens forholdsmessighet at det kun er data om omstendighetene rundt kommunikasjon, ikke om innholdet i kommunikasjonen som skal lagres. Innholdet i samtaler, SMS eller e-post skal altså ikke lagres, ei heller hvilke nettsteder man har besøkt. At trafikkdata er mindre sensitivt enn innholdsdata reflekteres i forskjellene i kriminalitetskravet for henholdsvis innhenting av trafikkdata og gjennomføring av kommunikasjonsavlytting. Det er også lagt til grunn i EMD-praksis, jf. P.G. og J.H. mot Storbritannia (dom 25.september 2001, saksnr. 44787/98) avsnitt 83-84.»

Datatilsynet, Advokatforeningen, Institutt for informatikk ved Universitetet i Oslo, Elektronisk Forpost Norge, Stopp datalagringsdirektivet Tromsø og Trondheim («Folkets høringsuttalelse«), Troms Nei til EU, IKT Norge og *Den internasjonale juristkommisjonen (avdeling Norge)* mener at gjennomføringen av datalagringsdirektivet vil krenke EMK artikkel 8, dog med noe ulik grad av sikkerhet. Advokatforeningen uttaler for eksempel at den foreslåtte gjennomføringen «mest sannsynlig» vil være i strid med EMK artikkel 8. Sentralt for disse høringsinstansene er at inngrepet ikke kan anses rettferdiggjort etter EMK artikkel 8 nr. 2.

Både *Den internasjonale juristkommisjonen* (avdeling Norge) og *Datatilsynet* presiserer uttrykkelig at det som først og fremst må vurderes er om selve lagringen av opplysningene kan rettferdiggjøres etter EMK artikkel 8 nr. 2. *Den internasjonale juristkommisjonen (avdeling Norge)* viser i den forbindelse til Europarådets konvensjon 20. januar 1981 nr. 108 om personvern i forbindelse med elektronisk behandling av personopplysninger (persondatakonvensjonen), EU-direktiv 1995/46/EF om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger (personopplysningsdirektivet), EU-direktiv 2002/58/EF om behandling av personopplysninger og beskyttelse av privatlivets fred i den elektroniske kommunikasjonssektor (kommunikasjonsdirektivet) og anbefaling R (87) 15 fra Europarådets ministerkomité om bruk av persondata i politisektoren. Det hevdes at datalagringsdirektivet bryter med selve grunnforutsetningen i disse instrumentene:

> «[…] selve registreringen og lagringen av personopplysninger – selv når det skjer i henhold til avtale mellom vedkommende person og for eksempel tilbyder av teletjenester – skal begrenses i omfang og tid til det som er strengt nødvendig for gjennomføring av tjenesten og administrasjon av kundeforholdet. Deretter skal opplysningene slettes.»

De fleste høringsinstansene som mener datalagringsdirektivet er i strid med EMK artikkel 8 viser

til at det i høringsnotatet ikke er dokumentert at datalagringen er nødvendig for å avdekke, etterforske og straffeforfølge den type kriminalitet som er foreslått omfattet, og at lagringen uansett ikke er forholdsmessig ettersom den er svært inngripende. Mange av disse høringsinstansene erkjenner imidlertid at EMD ikke har tatt stilling til et tilsvarende spørsmål, men hevder at den foreliggende rettspraksis likevel må tas til inntekt for at inngrepet ikke er forenelig med EMK artikkel 8. Den internasjonale juristkommisjonen viser blant annet til EMDs avgjørelser *Weber og Saravia mot Tyskland*, 29. juni 2006 (nr. 54934/00), *Liberty m.fl. mot Storbritannia*, 1. juli 2008 (nr. 58243/00), og *S og Marper mot Storbritannia (storkammer)*, 4. desember 2008 (nr. 30562/04 og 30566/04), og oppsummerer slik:

> «Kombinasjonen av denne avgjørelsen [S og Marper mot Storbritannia] og EMDs praksis vedrørende diverse former for kommunikasjonskontroll og annen behandling av kommunikasjonsdata, viser at ikke-målrettet, tvangsmessig og generell masselagring av alminnelige borgeres personopplysninger, uavhengig av noen konkret etterforskning, vil ha store problemer med å passere EMDs normale krav til proporsjonalitet.»

Flere av disse høringsinstansene etterlyser også en konkret vurdering av hvilke mindre inngripende tiltak som er vurdert.

Enkelte høringsinstanser som mener datalagringsdirektivet er i strid med EMK artikkel 8 omtaler også betydningen av EMDs avgjørelse *K.U. mot Finland,* 27. juni 2006 (nr. 2872/02). De fleste legger til grunn at EMD i avgjørelsen bare vurderte spørsmålet om utlevering – ikke spørsmålet om lagringen av data – og konkluderer med at dommen ikke kan tas til inntekt for at staten kan være forpliktet til å registrere og oppbevare data.

Advokatforeningen viser særlig til at skjønnsmarginen når det gjelder å vareta den nasjonale sikkerhet og bekjempe kriminalitet vil være meget mindre enn det som anføres i høringsnotatet:

> «Skjønnsmarginen vil være mindre – og dermed EMDs kontroll av nødvendigheten mer inngående – når det er tale om inngrep som ikke kan knyttes til konkrete kriminelle handlinger, men kun tilrettelegger for fremtidig etterforskning. I tillegg kommer at EMD antageligvis vil føle seg særlig kallet til å sette opp strenge kriterier for å tillate generell overvåkning av befolkningen, hvilket jo kan tenkes misbrukt av myndighetene, særlig dem med svakere demokratisk forankring. Dette vil være en alvorlig trussel mot den frihet konvensjonen skal sikre.»

Advokatforeningen viser også til at statene må vise at det er tilstrekkelig vern mot misbruk, noe som må omfatte adgang til å kontrollere opplysninger som er lagret om seg selv og til å korrigere disse om nødvendig.

IKT Norge mener uttalelsen i høringsnotatet om at lagringsplikten i direktivet representerer «et mindre inngripende inngrep for den enkelte enn for eksempel telefonavlytting […]» og «at dette [lagringen] ikke vil gjelde informasjon som er direkte knyttet til folks identitet», er uriktig:

> «Vi lever en stadig større del av våre liv på en måte som innebefatter bruk av teknologi. Mer og mer av vår kommunikasjon med omverdenen foregår ved hjelp av elektronisk kommunikasjon. Disse teknologitrendene vil øke i årene som kommer. Det vil stilles krav om at vår kontakt med offentlige myndigheter i større grad skal foregå elektronisk. Våre kjøp av varer og tjenester vil i større grad foregå elektronisk og vår kommunikasjon med familie, venner og kolleger vil i større og større grad foregå elektronisk. I tillegg vil flere og flere av våre eiendeler selv knyttes opp mot elektronisk kommunikasjon 'the internet of things'. Alle disse teknologitrendene vil i sum gjøre at dette direktivet representerer det mest inngripende og altomfattende overvåkningsregimet i europeisk historie. Innholdet i og omfanget av data som samles inn vil i sum kunne gi et svært presist bilde av en persons identitet, historiske bevegelser og vil også kunne gi et ganske presist bilde av en persons framtidige bevegelser.»

Troms Nei til EU uttaler seg i samme retning:

> «Mest sannsynlig vil en profilanalyse av samtlige telekommunikasjonsmidler en person benytter i et halvt år være et langt sterkere inngrep i hans private sfære enn at et brev blir lest av uvedkommende.»

IKT Norge anfører også at uttalelsen i høringsnotatet om at «en praksis hvor kriminalitetsbekjempelse og varetakelse av den nasjonale sikkerhet beror på tilfeldigheter må i det lange løp betegnes som utilfredsstillende» beror på et skremmende samfunnssyn:

> «I et demokrati vil det aldri være slik at politiets etterforskning kan baseres på noen annet enn de 'tilfeldige' spor som til enhver tid finnes. Dersom analogien i resonnementet over skal være konsistent må det i så fall bety at en mener vi må innføre en lignende lagrings/overvåkningsplikt også for all annen informasjon som kan være nyttig for politiets etterforskning. I så fall beveger vi oss farlig nære grensen for å kunne kalle oss et demokratisk samfunn.»

NetCom, NITO, og *NorSIS* etterlyser en grundigere drøftelse av forpliktelsene som følger av EMK artikkel 8 uten at det tas stilling til om den foreslåtte gjennomføringen av datalagringsdirektivet vil være i strid med bestemmelsen.

Utenriksdepartementet har gitt en grundig gjennomgåelse av datalagringsdirektivets forhold til EMK artikkel 8. Som et utgangspunkt for vurderingene som foretas, viser Utenriksdepartementet til at det problematiske ved direktivet er at det er statene som pålegger tilbyderne en slik lagring:

> «Selv om direktivet pålegger en lagringsplikt som statene skal rette mot tilbydere av relevante telekommunikasjonstjenester, er det forholdet mellom myndighetene og brukerne av disse tjenestene som utløser personvernspørsmål. EMD har forutsatt at tjenestetilbyderes egen håndtering av slike data ikke berører retten til privatliv, se bl.a. Malone mot Storbritannia, saksnummer 8691/79, dom 2. august 1984, avsnitt 84, og P.G. og J.H. mot Storbritannia, saksnummer 44787/98, dom 25. september 2001, avsnitt 42. Tjenestetilbyderes innhenting og lagring av data for å ivareta forbrukerhensyn til kvalitetskontroll og korrekt fakturering må anses legitim så lenge uvedkommende hindres i å få tilgang til slike data. Det er derfor direktivets plikt til å lagre slike data for det angitte formålet – dvs. å sikre kompetente myndigheter tilgang til data på nærmere bestemte betingelser – som gjør det aktuelt å anse at det foreligger et inngrep i retten til privatliv. Dette henger sammen med at data kan gi informasjon om den individuelle bruken av slike tjenester dersom data sammenstilles med aktuell kundeinformasjon. Ved å koble opplysninger om bruken av telekommunikasjonstjenester og personlig identitet til brukeren av tjenesten, kan det indirekte gi informasjon som er vernet av retten til privatliv og korrespondanse. Det gjelder selv om innholdet i telefonsamtaler, e-post og annen digital kommunikasjon faller utenfor plikten til å lagre data. EMD har i avgjørelsen i P.G. og J.H. mot Storbritannia, i avsnittet referert ovenfor, likevel ansett at registrering av innholdsdata, f.eks. ved å avlytte en telefonsamtale, er et mer inngripende tiltak enn lagring av data.
>
> Direktivets pålegg om lagring av data er en konsekvens av den teknologiske utviklingen. Det antas i mindre utstrekning å være påkrevd for tilbydere av telekommunikasjonstjenester å lagre data for de angitte forbrukerrelaterte formål. Direktivet innebærer derfor i hovedsak at data som hittil er blitt lagret av tilbyderne av tjenester av forretningsmessige hensyn, fortsatt skal lagres på grunnlag av et annet hensyn, nemlig rettshåndhevende myndigheters evne til fortsatt kriminalitetsbekjempelse. EMD har ansett at slik lagring av data i sammenheng med potensiell tilgang til data for kompetente myndigheter utgjør et inngrep i henhold til artikkel 8, se i tillegg til de avgjørelser som er nevnt ovenfor, Amann mot Sveits saksnummer 27798/95, dom 16. februar 2000, avsnitt 69, og S. og Marper mot Storbritannia, saksnummer 30562/04 og 30566/04, dom 4. desember 2008, avsnitt 67. Dette gjelder uavhengig av om det faktisk kan godtgjøres at det er gitt tilgang til individuelle lagrede data, se Klass og andre mot Tyskland, saksnummer 5029/71, dom 6. september 1978, avsnitt 38 og 41, og Campbell mot Storbritannia, saksnummer 13590/88, dom 25. mars 1992, avsnitt 33. At bruken av telefontjenester er omfattet av artikkel 8 er klart, se bl.a. Craxi mot Italia, saksnummer 25337/94, dom 17. juli 2003, avsnitt 57. I dom 3. april 2007 i saken Copland mot Storbritannia, saksnummer 62617/00, bekreftet EMD at retten til privatliv også omfatter vern mot innsyn i e-post som sendes fra kontoradresse og personlig internettbruk (avsnitt 41).
>
> Direktivet er basert på den forutsetning at lagringsplikten som sådan er forenlig med EMK artikkel 8, særlig basert på erfaringer fra flere medlemsstater som viser at tiltaket er nødvendig for å bekjempe organisert kriminalitet og terrorisme, se fortalens punkt 9.»

Utenriksdepartementet viser videre til at plikten til å lagre data og betingelsene for myndighetenes tilgang til lagrede data må vurderes hver for seg i forhold til kriteriene i EMK artikkel 8 nr. 2. Om myndighetenes tilgang til de lagrede data uttales:

> «[…] slik tilgang [kan] bare være legitim så langt det er fastsatt i lov og det konkret er nød-

vendig og forholdsmessig for å ivareta et av de formål som er angitt i artikkel 8 (2). Direktivet overlater til medlemsstatene selv å fastsette nødvendige regler for tilgang til data, men utøvelsen av denne nasjonale kompetansen må skje innen de rammer som EMK artikkel 8 oppstiller, se direktivets fortale, punkt 25.»

3.2.2 Ytringsfrihet, herunder pressens kildevern og forsamlings- og foreningsfriheten

EMK artikkel 10 knesetter den enkeltes rett til ytringsfrihet:

«1. Enhver har rett til ytringsfrihet. Denne rett skal omfatte frihet til å ha meninger og til å motta og meddele opplysninger og ideer uten inngrep av offentlig myndighet og uten hensyn til grenser. Denne artikkel skal ikke hindre stater fra å kreve lisensiering av kringkasting, fjernsyn eller kinoforetak.
2. Fordi utøvelsen av disse friheter medfører plikter og ansvar, kan den bli undergitt slike formregler, vilkår, innskrenkninger eller straffer som er foreskrevet ved lov og som er nødvendige i et demokratisk samfunn av hensyn til den nasjonale sikkerhet, territoriale integritet eller offentlige trygghet, for å forebygge uorden eller kriminalitet, for å beskytte helse eller moral, for å verne andres omdømme eller rettigheter, for å forebygge at fortrolige opplysninger blir røpet, eller for å bevare domstolenes autoritet og upartiskhet.»

Også Grunnloven § 100 beskytter ytringsfriheten:

«Ytringsfrihed bør finde Sted.

Ingen kan holdes retslig ansvarlig for at have meddelt eller modtaget Oplysninger, Ideer eller Budskab, medmindre det lader sig forsvare holdt op imod Ytringsfrihedens Begrundelse i Sandhedssøgen, Demokrati og Individets frie Meningsdannelse. Det retslige Ansvar bør være foreskrevet i Lov.

Frimodige Ytringer om Statsstyrelsen og hvilkensomhelst anden Gjenstand ere Enhver tilladte. Der kan kun sættes slige klarlig definerede Grænser for denne Ret, hvor særlig tungtveiende Hensyn gjøre det forsvarligt holdt op imod Ytringsfrihedens Begrundelser.

Forhaandscensur og andre forebyggende Forholdsregler kunne ikke benyttes, medmindre det er nødvendigt for at beskytte Børn og Unge imod skadelig Paavirkning fra levende Billeder. Brevcensur kan ei sættes i Værk uden i Anstalter.

Enhver har Ret til Indsyn i Statens og Kommunernes Akter og til at følge Forhandlingerne i Retsmøder og folkevalgte Organer. Det kan i Lov fastsættes Begrænsninger i denne Ret ud fra Hensyn til Personvern og af andre tungtveiende Grunde.

Det paaligger Statens Myndigheder at lægge Forholdene til Rette for en aaben og oplyst offentlig Samtale.»

Borgerne har på den ene siden en frihet til å innhente, motta og formidle opplysninger. I enkelte situasjoner medfører ytringsfriheten at borgerne også har rett til å forholde seg taus. Pressen har for eksempel som utgangspunkt en rett til å holde seg taus om sine kilders identitet, noe som betraktes som en grunnleggende forutsetning for pressefriheten. I EMDs dom *Goodwin mot Storbritannia*, 27. mars 1996 (nr. 17488/90) avsnitt 39, uttalte EMD:

«Protection of journalistic sources is one of the basic conditions for press freedom, as is reflected in the laws and the professional codes of conduct in a number of Contracting States and is affirmed in several international instruments on journalistic freedoms […]. Without such protection, sources may be deterred from assisting the press in informing the public on matters of public interest. As a result the vital public-watchdog role of the press may be undermined and the ability of the press to provide accurate and reliable information may be adversely affected.»

I NOU 2009: 15 (kapittel 28.4 på side 334) legger Metodekontrollutvalget til grunn, under henvisning til EMDs avgjørelse *Nordisk Film & TV A/S mot Danmark*, 8. desember 2005 (nr. 40485/02), at kildevernet bare kan gjøres gjeldende der den som har formidlet informasjon til pressen bevisst opptrer som kilde, og der opplysningene er egnet til å avsløre kildens identitet.

Datalagringsdirektivet inneholder ikke regler som gjør inngrep i pressens rett til å forholde seg taus om sine kilders identitet. I praksis kan imidlertid direktivet oppfattes som en utfordring for kildevernet idet det foreskriver en systematisk lagring av all data. Konflikten mellom prinsippet om kildevern og kriminalitetsbekjempelse er ikke ny, jf. følgende redegjørelse hentet fra *høringsnotatet* kapittel 5:

«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.»

Mer omfattende lagring av data enn i dag kan også rent faktisk kan ha en dempende innvirkning på folks ytringsfrihet. Denne problemstillingen ble ikke berørt i høringsnotatet, men er problematisert av flere høringsinstanser. I forlengelsen av dette er det også av flere pekt på at denne «nedkjølende effekten» vil kunne påvirke forsamlings- og foreningsfriheten, jf. EMK artikkel 11 nr. 1 som lyder:

> «Enhver har rett til fritt å delta i fredelige forsamlinger og til frihet til forening med andre, herunder rett til å danne og slutte sg til fagforeninger for å verne sine interesser.»

Advokatforeningen, Institutt for informatikk ved Universitetet i Oslo, Universitetet i Bergen, Nei til EU Hordaland, Nei til EU Troms, Datatilsynet, Rødt, IKT Norge, Norsk presseforbund, Norsk journalistlag, Norsk redaktørforening, Norsk Informasjonssikkerhetslab (NISlab) ved Høgskolen i Gjøvik, Skribent- og ytringsfrihetsorganisasjonen Norsk PEN, Elektronisk Forpost Norge og *Den internasjonale juristkommisjonen (norsk avdeling),* mener at datalagringsdirektivet utfordrer ytringsfriheten, herunder kildevernet. *Den internasjonale juristkommisjonen* (norsk avdeling) fremhever at vernet om retten til fortrolig, privat kommunikasjon, som er beskyttet av EMK artikkel 8, er nært for-

bundet med ytringsfriheten. Det vises for det første til at borgernes rett til å kommunisere fritt seg imellom er en forutsetning for den enkeltes selvutfoldelse som individ, herunder bruk av ytringsfriheten. Kommisjonen viser videre særlig til at rettmessig varsling om kritikkverdige forhold og pressens kildevern kan bli skadelidende dersom datalagringsdirektivet gjennomføres i norsk rett.

Datatilsynet og *Rødt* er bekymret for direktivets negative effekt på forsamlings og foreningsfriheten. *Rødt* uttaler:

> «Det kan også være en potensiell trussel mot den frie forsamlingsretten, da det blir kartlagt hvor man befinner seg om man for eksempel har med og bruker en mobiltelefon. Når man vet at dette blir kartlagt, kan det heve terskelen for å delta på aktiviteter.»

Norsk presseforbund uttaler:

> «Den form for massetvangslagring av kommunikasjonsdata som Datalagringsdirektivet krever, reiser altså både pressefaglige og juridiske spørsmål om respekten for pressens kildevern, slik denne er beskyttet blant annet av EMK artikkel 8 og 10.
>
> […]
>
> Essensen i dette er at statlige inngrep i kommunikasjon mellom pressens kilder og pressen skal holdes på et absolutt minimumsnivå og at de bare unntaksvis kan aksepteres. Enten fordi inngrepet skjer som en utilsiktet, uunngåelig konsekvens av et generelt tiltak som for øvrig er nødvendig i et demokratisk samfunn for å ivareta andre legitime formål. I slike tilfeller skal det foreligge rettssikkerhetsgarantier mot at informasjonen blir brukt. Eller fordi det i seg selv anses som nødvendig i et demokratisk samfunn å bruke tvangsmidler for å avsløre en konkret kildes identitet. Avgjørelsene fra EMD – ikke minst Financial Times m fl mot Storbritannia – viser også at alene risikoen for at en kilde kan bli avslørt, og den «chilling effect» dette kan ha på kommunikasjon mellom potensielle kilder og pressen, anses som nok til at artikkel 10 kan være krenket. EMK verner således selve tilliten til at kildevernet er reelt.
>
> […]
>
> Med et system hvor kommunikasjonsdata fra alle praktiske kommunikasjonsformer mellom pressens kilder og pressen blir tvangsregistrert og lagret, vil det åpenbart kunne svekke potensielle kilders vilje til å gi pressen informasjon som er nødvendig for at pressen skal kunne utøve sin samfunnsoppgave.»

Norsk journalistlag viser til at kildevernreglene er lovmessige unntak fra prinsippet om fri bevisførsel og den alminnelige forklarings- og bevisplikten, og oppstiller begrensninger i adgangen til å føre bevis. Det innebærer at journalister ikke trenger å fortelle retten og myndighetene hvem deres anonyme kilder er. Det vises til at retten til å nekte å oppgi kildens identitet gjelder ikke bare situasjoner der kildens opplysninger er blitt publisert i massemediene, men også der disse kun har gitt journalister bakgrunnsinformasjon. Det pekes på at det kan være ulike grunner til at kilder ikke ønsker å tre frem i offentlighetens søkelys, og at undersøkelser viser at det finnes flest anonyme kilder innenfor utenriks- og kriminalstoff:

> «Åpne kilder kan for det første løpe en risiko med hensyn til sin egen arbeidssituasjon. Informanten vil for eksempel varsle om kritikkverdig forhold på arbeidsplassen som allmennheten bør vite om, men er engstelig for negative reaksjoner fra arbeidsgiver eller kollegaer. Det kan for det andre være at informasjonen som anonyme kilder gir til en representant for pressen, er et brudd på yrkesmessig taushetsplikt, som blant annet kan gi grunnlag for avskjed, straff- eller erstatningsansvar. Informasjonen kan like fullt ha samfunnsmessig betydning. Kildene kan for det tredje frykte represalier og hevn ved åpent å gi ut informasjon om kriminelle miljøer.»

Norsk journalistlag peker videre på at politi- og påtalemyndighet, domstolene, og andre kan ha interesse av å finne ut hvem kilden er, og hva som har blitt sagt til pressen:

> «Det kan vise seg at kildens informasjon har interesse for oppklaringen av et mulig straffbart forhold eller for saksforholdet i en sivil sak, og retten eller sakens parter ønsker kunnskap om kildens identitet. Dette kan blant annet gi grunnlag for å vurdere opplysningenes holdbarhet, for å få vedkommende kilde til å avgi ytterligere forklaring, eller være aktuelt fordi kilden mistenkes for et straffbart forhold eller for å ha gitt uriktige opplysninger, jf. Ot.prp. nr. 55 (1997-98) s. 10. «

Advokatforeningen uttaler at datalagringsdirektivet vil utgjøre et inngrep i pressens kildevern ved at det ikke gjøres unntak for lagring av data fra

redaksjonslokaler. *Institutt for informatikk ved Universitetet i Oslo* legger til grunn at kildevernet svekkes dersom datalagringsdirektivet gjennomføres. Det må derfor innføres bestemmelser som ikke bare beskytter redaksjonslokalene og journalisters utstyr mot beslag, men også mot utlevering av data om kommunikasjon til og fra journalister og avisredaksjoner. *Universitetet i Bergen* uttaler:

> «[…] det er ikke mulig å trekke et slikt klart skille mellom data hos kilden og informasjon hos pressen hvis man skal bruke transaksjonsdata i etterforskningen. En aktuell situasjon vil være at en historie i mediene inneholder opplysninger fra en anonym kilde, som indikerer straffbart brudd på taushetsplikten. Problemet oppstår dersom man ikke har en konkret mistanke til hvem kilden kan være. Hvis man i et slikt tilfelle skal bruke av transaksjonsdata til å finne kilden, må man analysere journalistens kontakt med mange personer over en lang tid for å komme videre. Da går man inn i informasjonen på en måte som ikke synes bare marginalt forskjellig fra å be journalisten selv oppgi kilden. Det vil også lett kunne svekke tilliten til medienes kildevern, og på sikt redusere tilfanget av kilder.»

Politijuristene er derimot kritiske til at datalagringsdirektivet skal gjøre inngrep i ytringsfriheten, herunder pressens kildevern i særlig grad. De uttaler:

> «Politijuristene kan ikke se at datalagring vil utgjøre noen praktisk forskjell for arbeidsrommet til norske journalister, og at spørsmålet om pressens kildevern i tilfelle bør utredes separat. At myndighetene kan fange opp kommunikasjon mellom journalister og deres anonyme kilder er ikke noe nytt. Virkeligheten er at dette kan gjøres allerede i dag, dersom det foreligger en pågående kommunikasjonskontroll rettet mot den person som viser seg å være en kilde til pressen. Etter det vi er kjent med har ikke dette vist seg å være et praktisk problem i dag. Er kildene beskyttet, vil politiet ikke kunne bruke eventuelle data som bevis, og vil også risikere avskjæring allerede på beslagstidspunktet. Vi konstaterer også at de mange negative spådommene om datalagring som er framsatt, ikke synes å ha inntrådt i eksempelvis Danmark og Nederland, som begge var tidlige med å innføre datalagring. Dette gjelder alt fra kostnadsnivået for teletilbyderne til mulige inngrep i pressefriheten.»

Kulturdepartementet viser til at det i Ot.prp. nr. 55 (1997-1998) og i St.meld. nr. 26 (2003-2004) er drøftet om det bør innføres et etterforskningsforbud mot pressens kilder. Kulturdepartementet viser også til at Medieansvarsutvalget har fått i oppdrag å vurdere særlige lovregler om anonymitetsrett og etterforskningsforbud mot kilder, forefattere, opphavsmenn eller lignende.

3.2.3 Uskyldspresumsjonen

I EMK artikkel 6 om retten til en rettferdig rettergang, heter det i nr. 2:

> «Enhver som blir siktet for en straffbar handling, skal antas uskyldig inntil skyld er bevist etter loven.»

Uskyldspresumsjonen er også inntatt i andre folkerettslige instrumenter, blant annet SP artikkel 14 nr. 2.

Datalagringsdirektivets forhold til uskyldspresumsjonen ble ikke omtalt i høringsnotatet.

Uskyldspresumpsjonen utgjør for det første en bevisbyrderegel. Det er påtalemyndigheten som må føre bevis for tiltaltes skyld i straffesaker. Det er noe omstridt hvor langt kravet også medfører at det må anvendes et strengt beviskrav i straffesaker, se for eksempel Rt. 2008 side 1409. Dernest utgjør uskyldspresumsjonen en skranke for hvilke uttalelser offentlige myndigheter kan avgi som impliserer skyld før skyldspørsmålet er avgjort av en domstol. Etter en frifinnende dom vil det videre kunne være i strid med uskyldspresumsjonen å behandle den frifunne som om han likevel er skyldig. For det tredje stiller bestemmelsen visse materielle krav til hvordan straffebestemmelser må utformes.

FriBit, Elektronisk Forpost Norge, Skribent- og ytringsfrihetsorganisasjonen Norsk PEN og *Stopp datalagringsdirektivet Tromsø og Trondheim/«Folkets høringsuttalelse»* anfører at datalagringsdirektivet er i strid med uskyldspresumpsjonen. Det gjør også *Datatilsynet:*

> «Datatilsynet mener datalagringen i henhold til direktivet kan ses som en forskuttert etterforskningsmetode, som skal kunne tas i bruk før gjeldende vilkår for å ta i bruk ordinære metoder er oppfylt. At staten iverksetter etterforskningstiltak som retter seg mot hele samfunnet, uten at det foreligger mistanke mot noen, og før det engang er identifisert et mulig lovbrudd, innebærer et paradigmeskifte i norsk strafferettstradisjon og kan ses som et uttrykk for at hele folket settes under mistanke.»

Skribent- og ytringsfrihetsorganisasjonen Norsk PEN utdyper sitt syn slik:

> «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. Dette er å snu dagens rettsorden fullstendig på hodet; Her gjelder ikke lenger at en borger er uskyldig inntil det motsatte er bevist. Nå er argumentet at den enkelte borger trenger datalagringen, slik at de hele tiden selv vil være sikret å kunne legge fram bevis på sin uskyld. Norsk PEN vil advare mot å begrunne et etterforskningstiltak rettet mot hele samfunnet med en argumentasjon som ikke lenger legger til grunn prinsippet om at en borger er å anse som uskyldig inntil det motsatte er bevist utenfor rimelig tvil.»

FriBit uttaler:

> «Rettsstaten vår bygger på prinsippet om at man er uskyldig til det motsatte er bevist. I dette ligger at man heller ikke skal etterforskes med mindre man er mistenkt for å planlegge, medvirke til eller ha begått en kriminell handling. Prinsippet om uskyldspresumpsjon står sterkt både i borgernes rettsoppfatning og i Europas Menneskerettighetskonvensjon. Innføringen av DLD vil føre til en innsamling av data om alle landets borgere uten å ta hensyn til hvorvidt de er mistenkte eller ikke. Det å snu rundt på uskyldspresumpsjonen vil føre til en rekke uheldige konsekvenser, deriblant en endring av folks atferdsmønster (chilling effect), en forskjøvet balanse mellom det offentlige og private, samt en bevegelse mot en nasjon basert på mistillit framfor tillit – der man må bevise sin uskyld ved enhver korsvei.»

3.2.4 Øvrige forpliktelser

Enkelte av høringsinstansene tok også opp forholdet til SP og FNs barnekonvensjon som begge er gjort til en del av norsk rett ved menneskerettsloven.

SP artikkel 17 lyder:

> «1. Ingen må utsettes for vilkårlige eller ulovlige inngrep i privat- eller familieliv, hjem eller korrespondanse, eller ulovlige inngrep på ære eller omdømme.
> 2. Enhver har rett til lovens beskyttelse mot slike inngrep eller angrep. «

FNs barnekonvensjon artikkel 16 lyder:

> «1. Ingen barn skal utsettes for vilkårlig eller ulovlig innblanding i sitt privatliv, sin familie, sitt hjem eller sin korrespondanse, eller for ulovlige angrep mot sin ære eller sitt omdømme.
> 2. Barnet har rett til lovens beskyttelse mot slik innblanding eller slike angrep.»

Også FNs barnekonvensjonen artikkel 34 kan ha relevans:

> «Partene påtar seg å beskytte barnet mot alle former for seksuell utnytting og seksuelt misbruk. For dette formål skal partene særlig treffe alle egnede nasjonale, bilaterale og multilaterale tiltak for å hindre at noen:
> a. tilskynder eller tvinger et barn til å delta i enhver form for ulovlig seksuell aktivitet,
> b. utnytter barn ved å bruke dem til prostitusjon eller andre ulovlige seksuelle handlinger,
> c. utnytter barn ved å bruke dem i pornografiske opptredener eller i pornografisk materiale.»

Politiets sikkerhetstjeneste (PST) uttaler seg om positive menneskerettighetsforpliktelser som varetar offerets rettsvern:

> «Implementering av direktivet er nødvendig i forhold til å sikre en effektiv etterlevelse av de internasjonale konvensjoner om terrorbekjempelse som Norge er bundet av. Uten bestemmelser som sikrer tilgang til trafikkdata vanskeliggjøres for eksempel oppfølgningen av de nye straffebestemmelser om oppfordring, opplæring og rekruttering til terrorvirksomhet da svært mye av denne aktiviteten foregår på Internett. Uten lagring av trafikkdata vil den nye strl. § 147 c også ha liten betydning i praksis.
>
> Avslutningsvis vil vi også peke på den forpliktelse Den europeiske menneskerettighetsdomstol har fremhevet om at statene skal sikre fornærmedes rettigheter når det gjelder at den skyldige skal kunne finnes og straffes. Uten data vil denne rettighet i mindre grad kunne ivaretas.»

Kripos mener datalagring er helt nødvendig for å kunne etterforske blant annet internettrelaterte seksuelle overgrep. I den forbindelse viser Kripos også til at en gjennomføring av datalagringsdirektivet synes å være en forutsetning for at Norge skal kunne vareta sine forpliktelser etter FNs barnekonvensjon artikkel 34.

Utenriksdepartementet viser til at det prinsipielt er mulig å anse at direktivet er forenlig med gjeldende menneskerettigheter, samtidig som innholdet i og den konkrete anvendelse av nasjonale gjennomføringsbestemmelser til direktivet potensielt kan resultere i krenkelse av de samme forpliktelser. Det vises også til at det ikke kan utelukkes at mer presis europeisk lovgivning om datalagring vil kunne påvirke vurderingen av de krav til klarhet og forutberegnelighet i nasjonal rett som følger av gjeldende menneskerettsforpliktelser.

Som særlig relevante bestemmelser viser Utenriksdepartementet til EMK artikkel 8, SP artikkel 17 og FNs barnekonvensjon artikkel 16. Innenfor alle bestemmelsene må det foretas en avveining av hensynet til effektiv kriminalitetsbekjempelse og varetakelse av personvernet. Utenriksdepartementet legger videre til grunn at SP artikkel 17 pålegger forpliktelser som langt på vei er sammenfallende med EMK artikkel 8.

Utenriksdepartementet peker også på. General Comment nr. 16 (1988) fra FNs menneskerettighetskomité, som understreker statens ansvar for å treffe effektive tiltak for å hindre at borgerne krenker hverandres privatliv (avsnitt 1 og 9), og faktaark nr. 32 fra FNs Høykommissær for menneskerettigheter side 45-46. FNs barnekonvensjon artikkel 16 har en tilsvarende bestemmelse om barns vern mot krenkelse av privatlivet.

3.3 Departementets vurderinger

3.3.1 Innledning

Det er særlig to forhold ved gjennomføringen av datalagringsdirektivet som kan være problematisk i forhold til ulike menneskerettslige forpliktelser som Norge er bundet av; den statlig pålagte lagringsplikten, og politiets og påtalemyndighetens senere tilgang til og bruk av de lagrede opplysningene. Disse kan ikke vurderes helt uavhengig av hverandre.

Den myndighetspålagte lagringsplikten og kompetente myndigheters senere tilgang til og bruk av de lagrede opplysningene, kan medføre inngrep i retten til privatliv og korrespondanse, jf. EMK artikkel 8 nr. 1. Inngrepet må da rettferdiggjøres etter EMK artikkel 8 nr. 2, noe som innebærer at inngrepet må ha hjemmel i lov, oppfylle et legitimt formål, og være nødvendig i et demokratisk samfunn for å oppfylle det legitime formålet.

En myndighetspålagt lagringsplikt uten tilknyttede regler om datasikkerhet og om tilgang til opplysningene, vil være et meget mer alvorlig inngrep enn en myndighetspålagt lagringsplikt som samtidig stiller opp strenge regler om datasikkerhet, tilgang, bruk og sletting av opplysningene. Slike forhold har blant annet betydning i vurderingen av om den pålagte lagringen anses nødvendig i et demokratisk samfunn for å oppfylle et legitimt formål. Dersom inngrepet på den annen side vurderes fra det tidspunkt politi eller påtalemyndighet eventuelt får tilgang til lagrede opplysninger, vil det kunne være av betydning at politi og påtalemyndighet får tilgang på bakgrunn av en myndighetspålagt lagringsplikt, i motsetning til for eksempel opplysninger som er lagret etter en frivillig inngått avtale mellom private parter. Vurderingen i et konkret tilfelle av om tilgangen til opplysningene er nødvendig i et demokratisk samfunn for å oppfylle et legitimt formål, vil da påvirkes av hvilke regler om tilgangen som er fastsatt, herunder også regler som skal forhindre misbruk og regler om sletting av opplysninger som eventuelt viser seg ikke å være nødvendige for å oppnå formålet.

Tilsvarende vurderinger av inngrepets art og forholdsmessighet vil måtte foretas etter andre menneskerettslige forpliktelser som Norge er bundet av. Det gjelder for eksempel EMK artikkel 10 (ytringsfrihet), EMK artikkel 11 (forsamlings- og foreningsfrihet), SP artikkel 17 og FNs barnekonvensjon artikkel 16.

Direktivet forutsetter en nasjonal gjennomføring. Det er denne nasjonale gjennomføringen av datalagringsdirektivet som i konkrete og individuelle tilfeller eventuelt kan krenke ulike menneskerettigheter som nasjonalstatene er bundet av.

3.3.2 Retten til privatliv (EMK artikkel 8)

3.3.2.1 Noen utgangspunkter

EMK artikkel 8 nr. 1 beskytter mot inngrep fra staten i retten til privatliv, familieliv, hjem og korrespondanse. Denne beskyttelsen er imidlertid ikke absolutt. Offentlige myndigheter kan gripe inn i retten etter EMK artikkel 8 nr. 1 dersom det er fastsatt i lov og nødvendig i et demokratisk samfunn for å vareta ett eller flere legitime formål, jf. EMK artikkel 8 nr. 2.

Det foreligger omfattende praksis fra EMD om tolkningen av EMK artikkel 8. Denne praksisen er av avgjørende betydning for hvordan vilkårene i bestemmelsen skal forstås. EMD har imidlertid aldri tatt stilling til et tilfelle som er direkte sammenlignbart med den situasjonen som gjennomføringen av datalagringsdirektivet medfører.

Vurderingen av hva som er nødvendig i et demokratisk samfunn for å vareta ett eller flere legitime formål, er videre skjønnsmessig og beror på en konkret avveining av en rekke ulike hensyn. Gjennomføringen av datalagringsdirektivet fordrer særlig en avveining av hensynet til personvern og hensynet til hvilke virkemidler som er nødvendige for å bekjempe alvorlig kriminalitet. Begge hensynene er i et demokratisk samfunn åpenbart legitime. Avveiningen og vektleggingen av slike hensyn vil kunne variere i takt med samfunnsutviklingen for øvrig. EMD har for eksempel gjentatte ganger uttalt at EMK er et «living instrument» som må tolkes i lys av «the present day conditions», jf. for eksempel EMDs dom *Tyrer mot Storbritannia*, 25. april 1978 (nr. 5856/72) avsnitt 31. Ved avveiningen av slike hensyn i lys av samfunnsutviklingen, er det derfor mulig å komme til ulike resultater. Dette har kommet tydelig til uttrykk i høringen, hvor særlig representantene for politi og påtalemyndighet har argumentert for at den foreslåtte gjennomføringen av datalagringsdirektivet er i samsvar med EMK artikkel 8, mens særlig representantene for deler av det sivile samfunn har argumentert for at forslaget er i strid med EMK artikkel 8.

3.3.2.2 Inngrep i retten til privatliv og korrespondanse

Som i høringsnotatet legger departementet til grunn at både den myndighetspålagte lagringsplikten og politiets og påtalemyndighetens tilgang til opplysningene i senere konkrete saker kan utgjøre inngrep i retten til privatliv og korrespondanse etter EMK artikkel 8 nr. 1. Dette har også de fleste av høringsinstansene som uttaler seg om EMK artikkel 8 lagt til grunn.

Vedrørende den myndighetspålagte lagringsplikten, viser departementet til EMDs dom *Leander mot Sverige,* 26. mars 1987 (nr. 9248/81). Dommen kan hevdes å gi uttrykk for at all lagring av opplysninger som staten selv foretar og som vedrører enkeltmenneskers privatliv, utgjør et inngrep i retten til privatliv, slik denne er beskyttet etter EMK artikkel 8 nr. 1. Departementet legger til grunn at det samme vil gjelde også for en myndighetspålagt lagringsplikt. At den myndighetspålagte lagringen kan utgjøre et inngrep i EMK artikkel 8 nr. 1, synes også forutsatt i datalagringsdirektivet artikkel 4 og fortalen punkt 9 og 25.

Det følger forutsetningsvis av datalagringsdirektivet at den senere utleveringen til politi og påtalemyndighet i konkrete saker kan utgjøre et inngrep i retten til privatliv og korrespondanse, jf. særlig artikkel 4 og fortalen punkt 9 og 25. EMD har i flere avgjørelser slått fast at politiets innhenting og bruk av personlige opplysninger kan utgjøre inngrep etter EMK artikkel 8 nr. 1, se for eksempel *Malone mot Storbritannia*, 2. august 1984 (nr. 8691/79) og *P.G. og J.H. mot Storbritannia*, 25. september 2001 (nr. 44787/98).

Spørsmålet blir så om inngrepene kan rettferdiggjøres under henvisning til EMK artikkel 8 nr. 2. Inngrepene må da ha hjemmel i lov, ha til hensikt og være egnet til å oppfylle et eller flere legitime formål, og være nødvendig i et demokratisk samfunn for å oppfylle de legitime formålene.

3.3.2.3 Lovhjemmel

Det er først og fremst opp til nasjonale myndigheter å avgjøre om inngrepet har hjemmel i nasjonal rett. EMD stiller imidlertid krav til at den nasjonale hjemmelen oppfyller visse grunnleggende rettsstatsprinsipper. I EMDs dom *S og Marper mot Storbritannia* (storkammer), 4. desember 2008 (nr. 30562/04 og 30566/04) avsnitt 95, uttrykkes dette slik:

> «The law must thus be adequately accessible and foreseeable, that is, formulated with sufficient precision to enable the individual – if need be with appropriate advice – to regulate his conduct. For domestic law to meet these requirements, it must afford adequate legal protection against arbitrariness and accordingly indicate with sufficient clarity the scope of discretion conferred on the competent authorities and the manner of its exercise»

Kravene til klarhet og presisjon vil kunne variere noe etter omstendighetene, blant annet etter hvor alvorlig inngrepet er. I *Malone mot Storbritannia* 2. august 1984 (nr. 8691/79) avsnitt 67, uttalte EMD:

> «[…] the requirements of the Convention, notably in regard to foreseeability, cannot be exactly the same in the special context of interception of communications for the purposes of police investigations as they are where the

> object of the relevant law is to place restrictions on the conduct of individuals. In particular, the requirement of foreseeability cannot mean that an individual should be enabled to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly. Nevertheless, the law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to this secret and potentially dangerous interference with the right to respect for private life and correspondence.»

I *Kruslin mot Frankrike*, 24. april 1990 (nr. 11801/85) avsnitt 33, uttalte EMD videre:

> «Tapping and other forms of interception of telephone conversations represent a serious interference with private life and must accordingly be based on a 'law' that is particularly precise. It is essential to have clear, detailed rules on the subject, especially as the technology available for use is continually becoming more sophisticated.»

Både reglene om lagring og reglene om kompetente myndigheters tilgang til de lagrede opplysningene må tilfredsstille kravene til tilgjengelighet, klarhet og presisjon. Departementets forslag til endringer i ekomloven, straffeprosessloven og verdipapirhandelloven er uformet med sikte på å sikre at kravene til tilgjengelighet, klarhet og presisjon blir varetatt.

3.3.2.4 Formålsmessighet

Formålet med lagringsplikten, og den tilknyttet tilgangen til opplysningene for politi og påtalemyndighet er å bekjempe alvorlig kriminalitet, vareta andres rettigheter og friheter, og i sin ytterste konsekvens vareta den nasjonale sikkerheten. Ved bekjempelse av kriminalitet varetas ikke bare samfunnets interesse i at kriminalitet blir straffet, men også konkrete rettigheter til øvrige enkeltindivider – særlig ofrene for kriminalitet. Dette er et aspekt ved strafferettspleien som får stadig større oppmerksomhet innenfor arbeid med menneskerettighetene. Innenfor Europarådet er det blant annet opprettet en arbeidsgruppe som skal utarbeide retningslinjer for hvordan man kan etterforske og sørge for at alvorlige menneskerettsbrudd ikke forblir ustraffet (Committee of experts on impunity – DH-I).

Formålene om å bekjempe alvorlig kriminalitet og vareta den nasjonale sikkerheten og andres rettigheter, er legitime formål etter EMK artikkel 8 nr. 2.

3.3.2.5 Nødvendighet

Kravet om at inngrepet må være nødvendig i et demokratisk samfunn for å vareta et legitimt formål, gir uttrykk for at det må foretas en konkret interesseavveining mellom inngrepet i privatlivet og de legitime formålene. EMD uttrykte dette slik i *Olsson mot Sverige*, 24. mars 1988 (nr. 10465/83) avsnitt 67:

> «the notion of necessity implies that the interference corresponds to a pressing social need and, in particular, that it is proportionate to the legitimate aim pursued»

Sitatet kan gi uttrykk for at det må foretas en toleddet vurdering, slik at det først må avgjøres om det foreligger et «pressing social need», og deretter foretas en konkret forholdsmessighetsvurdering mellom inngrepet og de legitime formålene. Men EMD vurderer ofte ikke isolert om det foreligger et presserende samfunnsmessig behov. Den første delen av sitatet kan da langt på vei hevdes å være et navn på resultatet: Dersom inngrepet er nødvendig, foreligger det et presserende samfunnsmessig behov for å foreta inngrepet, og motsatt, dersom inngrepet ikke er nødvendig, foreligger ikke et slikt behov.

Det er på det rene at det foreligger et presserende samfunnsmessig behov for å bekjempe alvorlig kriminalitet. Departementet anser at tilgang til data kan være av avgjørende betydning for at en rekke straffbare og ulovlige handlinger oppklares. Dette ble også lagt til grunn av EU under vedtagelsen av datalagringsdirektivet, og er fremhevet særlig av politi og påtalemyndigheten under høringen, jf. kapittel 5 om politiets behov.

Under enhver omstendighet må det foretas en konkret forholdsmessighetsvurdering mellom inngrepet og de legitime hensynene som inngrepet skal vareta.

I denne vurderingen vil statene ha en skjønnsmargin («margin of appreciation«). Hvor stor skjønnsmargin statene tilkjennegis, varierer fra sak til sak. At statene tilkjennegis en skjønnsmargin, er dels en erkjennelse av at statene kan være nærmere enn EMD til å vurdere betydningen og virkningen av enkelte forhold. Statene vil blant annet kunne være nærmere enn EMD til å avveie hvordan store og tunge motstridende samfunnsin-

teresser, som hver for seg er legitime, skal avveies mot hverandre. Det vil også kunne være av betydning om det finnes en felleseuropeisk regulering på området.

Som i høringsnotatet legger departementet til grunn at statene som utgangspunkt må ha en forholdsvis stor skjønnsmargin ved vurderingen av hvilke tiltak det er nødvendig å iverksette for å bekjempe alvorlig kriminalitet og vareta den nasjonale sikkerheten og andres rettigheter. Størrelsen på skjønnsmarginen er imidlertid ikke avgjørende for den forholdsmessighetsvurderingen departementet nå foretar.

Det kan tenkes en rekke faktorer som er av betydning i den konkrete forholdsmessighetsvurderingen. Et absolutt krav er at inngrepet må være egnet til å realisere formålet. Departementet anser at den myndighetspålagte lagringsplikten vil bidra til å bekjempe alvorlig kriminalitet, sikre andres rettigheter og vareta den nasjonale sikkerheten, jf. nærmere i kapittel 5 om politiets behov. En annen sak er at graden av måloppnåelse kan være av betydning i en mer konkret avveining mellom inngrepet og de legitime hensynene som begrunner inngrepet.

Inngrepet vil normalt ikke være forholdsmessig dersom formålet kan nås med lempeligere midler. Departementets utgangspunkt er imidlertid at muligheten for å bekjempe alvorlig kriminalitet i samfunnet vil svekkes dersom politi og påtalemyndighet ikke sikres tilgang til data, jf. nærmere under kapittel 5.5. Den tyske forfatningsdomstolen har lagt til grunn at formålet med inngrepet ikke like effektivt kan nås med lempeligere midler, jf. dom avsagt av den tyske forfatningsdomstolen (første senat) 2. mars 2010 i sakene 1 BvR 256/08, 1 BvR 263/08 og 1 BvR 586/08, avsnitt 208.

Hvorvidt gjennomføringen av datalagringsdirektivet vil tilfredsstille kravet til forholdsmessighet, må således bero på en mer konkret avveining av inngrepets styrke i forhold til de som rammes, vurdert opp mot de hensynene som tilsier inngrep.

EMD har ikke tidligere tatt stilling til om og under hvilke omstendigheter en generell myndighetspålagt lagringsplikt av data er nødvendig i et demokratisk samfunn for å bekjempe alvorlig kriminalitet og vareta den nasjonale sikkerheten og andres rettigheter. Departementet kan imidlertid ikke se at det skal være avgjørende for om den pålagte lagringsplikten er forholdsmessig. For det første må behovet for en slik generell myndighetspålagt lagringsplikt ses i lys av de gjeldende samfunnsforholdene. Her er det på det rene at stadig mer av den mellommenneskelige kommunikasjonen foregår ved bruk av ulike digitale og elektroniske virkemidler. Samtidig vil behovet for tilgang til data for å oppklare kriminalitet, øke. For det andre er det ingen av de generelle momentene som EMD har oppstilt som tilsier at en slik generell myndighetspålagt lagringsplikt som sådan vil være uforholdsmessig. EMD understreker derimot at det må foretas en konkret avveining av inngrepets styrke vurdert opp mot de hensynene som tilsier inngrep. I vurderingen av inngrepets styrke, kan det imidlertid være av betydning at det foreligger en generell myndighetspålagt lagringsplikt. Det må også være av vesentlig betydning om det foreligger tilfredsstillende rettssikkerhetsgarantier som kan forhindre vilkårlig tilgang til opplysningene. Dette er det samme utgangspunktet for forholdsmessighetsvurderingen som EU har kommet frem til, jf. datalagringsdirektivet artikkel 4 og fortalen kapittel 9 og 25. Også den tyske forfatningsdomstolen har lagt til grunn at den myndighetspålagte lagringsplikten som sådan ikke er i strid med den tyske forfatningen, såfremt særlig reglene om lagring og tilgang til opplysningene er tilfredsstilende, se dom avsagt av den tyske forfatningsdomstolen (første senat), 2. mars 2010 i sakene 1 BvR 256/08, 1 BvR 263/08 og 1 BvR 586/08, avsnitt 219. Departementet kan heller ikke se at EMDs dom S og Marper mot Storbritannia (storkammer), 4. desember 2008, nr. 30562/04 og 30566/04, tilsier at det må fastsettes et annet utgangspunkt for forholdsmessighetsvurderingen.

Både høringen og EUs lovgivningsprosess har vist at det kan være delte meninger om hvor inngripende den myndighetspålagte lagringen av data er for privatlivet. Det er redegjort nærmere for departementets syn på dette spørsmålet i kapittel 6 om personvern. Lagringstiden foreslås satt til 12 måneder, jf. kapittel 9. Politiet og påtalemyndighetens tilgang til opplysningene er foreslått begrenset til alvorlig kriminalitet samt enkelte nærmere bestemte lovbrudd som anses som særlig vanskelig å etterforske uten tilgang på data. Basestasjonssøk er særlig inngripende i personvernet og strafferammekravet er således foreslått satt høyere her enn ved utlevering av personspesifikk data. I begge tilfeller er utlevering underlagt domstolskontroll, jf. kapittel 12. Domstolen skal treffe beslutning ved kjennelse som innebærer en plikt til å begrunne beslutningen. Mistenkte skal underrettes om utleveringspålegg. Ved utsatt underretning skal det oppnevnes en offentlig advokat for å ivareta vedkommendes rettssikkerhet. Overskuddsinformasjon hos politi

og påtalemyndighet skal håndteres i samsvar med reglene i lov 28. mai 2010 nr. 16 om behandling av opplysninger i politiet og påtalemyndigheten (politiregisterloven). Loven har ikke trådt i kraft. Muligheten for å omgå disse vilkårene ved vitneforklaring i straffesaker eller begjæring om bevisfremleggelse i sivile søksmål, foreslås dessuten stengt.

Fra hovedregelen om at adgangen til data skal forbeholdes politi og påtalemyndighet, foreslås et unntak for Finanstilsynet, jf. nærmere under kapittel 14. Adgangen foreslås imidlertid endret sammenlignet med gjeldende rett slik at også tilsynet må be om rettslig kjennelse. Tilsynet skal dessuten heller ikke ha hastekompetanse med etterfølgende domstolsprøving eller adgang til å få utlevert basestasjonsutskrifter.

Disse vilkårene og begrensningene i retten til tilgang og bruk av data gir etter departementets oppfatning gode garantier mot vilkårlighet og maktmisbruk. Etter departementets oppfatning tilsier en konkret avveining av inngrepets styrke i forhold til de som rammes, vurdert opp mot de hensynene som tilsier inngrep, at inngrepet i privatlivet er nødvendig i et demokratisk samfunn for å bekjempe alvorlig kriminalitet, vareta den nasjonale sikkerheten og andres rettigheter.

3.3.3 Ytringsfrihet, herunder pressens kildevern og forsamlings- og foreningsfriheten

Det er særlig to forhold ved gjennomføringen av datalagringsdirektivet som kan tenkes å være problematisk for ytringsfriheten, herunder pressens kildevern. Det gjelder for det første den myndighetspålagte lagringen av data, og for det andre politiets og påtalemyndighetens mulige senere tilgang til disse opplysningene. I sin alminnelighet kan dette virke hemmende på den frie meningsytringen, og da kanskje særlig i det private rom. Dette er også påpekt av flere av høringsinstansene. Departementet legger imidlertid til grunn at den myndighetspålagte lagringen, sett i sammenheng med politiets og påtalemyndighetens senere tilgang til opplysningene, bare i svært begrenset grad vil ha en nedkjølende effekt på befolkningen i sin alminnelighet. Det vises blant annet til at det gjeldende regelverket hvor tilbyderne nærmest rutinemessig har lagret slike data, ikke synes å ha en slik dempende effekt på den frie meningsytringen. Det vises også til at det foreslås strenge regler om hvordan tilbyderne må lagre opplysningene, avgrenset lagringstid, begrenset tilgang til opplysningene for politi-, påtalemyndighet og Finanstilsynet samt domstolskontroll med at vilkårene overholdes. På samme vis som inngrepet i privatliv og korrespondanse må anses rettferdiggjort etter EMK artikkel 8 nr. 2, anser departementet at en eventuell dempende effekt på den frie meningsytringen i sin alminnelighet må anses rettferdiggjort etter EMK artikkel 10 nr. 2 av hensyn til å bekjempe alvorlig kriminalitet, vareta den nasjonale sikkerheten og andres rettigheter.

For det andre kan det tenkes at den myndighetspålagte lagringsplikten, tilgangen til opplysningene, eventuelt også senere bruk av opplysningene i for eksempel en rettssak, kan tenkes å utgjøre et inngrep i den særlige retten til å forholde seg taus som i enkelte situasjoner kan tenkes å være omfattet av ytringsfriheten. Det er her særlig pressens rett til å forholde seg taus om en kildes identitet (pressens kildevern) som har blitt fremhevet av høringsinstansene og i høringsnotatet.

I NOU 2009: 15 kapittel 28.5 og 28.6 (på side 335 til 339) har Metodekontrollutvalget vurdert generelt om kontroll av kommunikasjon mellom journalist og kilde og bevisføring av kildeavslørende materiale vil være i samsvar med ytringsfriheten.

Metodekontrollutvalget viser for det første til at EMD har ansett rettslige pålegg til journalister om å oppgi sin kilde, som inngrep i kildevernet. I saken *Goodwin mot Storbritannia*, 27. mars 1996 (nr. 17488/90), avsnitt 39, uttalte EMD:

> «Having regard to the importance of the protection of journalistic sources for press freedom in a democratic society and the potentially chilling effect an order of source disclosure has on the exercise of that freedom, such a measure cannot be compatible with Article 10 (art. 10) of the Convention unless it is justified by an overriding requirement in the public interest.»

For det andre viser utvalget til, under henvisning til EMDs avgjørelse *Roemen og Schmit mot Luxembourg*, 25. februar 2005 (nr. 51772/99), at ransaking av en journalists hjem og arbeidsplass utvilsomt utgjør et inngrep i retten til kildevern.

For det tredje legger utvalget til grunn, under henvisning til EMDs avgjørelse *Weber og Saravia mot Tyskland*, 29. juni 2006 (nr. 54934/00), at:

> «etterforskingsmetoder som rammer kommunikasjonen mellom journalist og kilde på en slik måte at kilders identitet kan avsløres eller som kan medføre at kilder blir mer tilbake-

> holdne med å formidle informasjon til pressen må anses som et inngrep i ytringsfriheten etter EMK artikkel 10. Dette må klart gjelde der journalisters og/eller redaksjoners kommunikasjonskanaler er avlyttet, men antakelig også der samtaler mellom journalist og kilde fanges opp som utilsiktet konsekvens av kommunikasjonskontroll rettet mot en mistenkt.»

Politiet og påtalemyndighetens samt Finanstilsynets tilgang til data, vil kunne medføre at pressens kilder avsløres – selv om pressen i utgangspunktet skulle ønske å holde identiteten til kilden hemmelig. Dette er en utilsiktet konsekvens av innhentingen av data men kan altså likevel tenkes å utgjøre et inngrep i ytringsfriheten etter EMK artikkel 10. Inngrepet må imidlertid antas å være større dersom det gis tilgang til data med den hensikt å avsløre en kilde, og særlig ved begjæring om tilgang til data som stammer fra pressens kommunikasjon.

På den annen side er ikke retten til ytringsfrihet, herunder pressens rett til kildevern, absolutt. Et inngrep i ytringsfriheten kan rettferdiggjøres etter EMK artikkel 10 nr. 2 dersom det er foreskrevet ved lov og er nødvendig i et demokratisk samfunn for å oppfylle ett eller flere legitime formål. Departementet anser at inngrepene har tilstrekkelig lovhjemmel og tar sikte på og er egnet til å oppfylle flere legitime formål.

Avgjørelsen av om inngrepene er nødvendig i et demokratisk samfunn for å bekjempe alvorlig kriminalitet, vareta den nasjonale sikkerheten og rettigheter til andre, må bero på en konkret vurdering av inngrepenes styrke målt opp mot de grunnene staten angir for å foreta inngrepene.

Som et utgangspunkt for vurderingen av inngrepenes styrke, slutter departementet seg til følgende utsagn fra Metodekontrollutvalget i NOU 2009: 15, kapittel 28.7, side 339:

> «Utvalget vil innledningsvis understreke at en fri og uavhengig presse er en grunnleggende forutsetning for informasjonsformidling, folkeopplysning og meningsdannelse i et demokrati. Særlig viktig er pressens bidrag til å avdekke kritikkverdige forhold og myndighetsmisbruk i samfunnet. For å utøve slik virksomhet er pressen avhengig av at enkeltmennesker som sitter på samfunnsmessig relevant informasjon tør videreformidle slik informasjon. I noen situasjoner kan dette bare skje i bytte mot et løfte om anonymitet, og kildevernet er dermed en forutsetning for at pressen skal kunne fylle rollen som «samfunnets vaktbikkje».
>
> Kildevernet berører altså både kildens rett til å formidle opplysninger, journalistens rett til å innhente opplysninger, journalistens rett til å formidle disse til samfunnet og borgernes rett til å motta opplysningene. Regler som beskytter pressens kildevern er dermed ikke gitt kun for å beskytte journalisten eller kilden, men også for å beskytte samfunnet, og borgernes mulighet til å motta den informasjon de trenger for å utøve sine demokratiske rettigheter.»

Pressens kildevern er således et svært viktig fundament i vårt demokratiske samfunn. Mange av høringsinstansene har hevdet at dette kildevernet vil bli illusorisk dersom pressens data alltid lagres, ettersom en kilde da ikke kan føle seg trygg på at politi eller påtalemyndighet ikke får viten om kildens kontakt med pressen. Det foreligger imidlertid heller ikke i dag noe alminnelig forbud mot at politiet igangsetter etterforskning mot en kilde eller en journalist ved mistanke om straffbare forhold. Et slikt forbud vil etter departementets oppfatning ganske klart medføre en uforholdsmessig begrensning i politiets plikt til å igangsette etterforskning av straffbare forhold, jf straffeprosessloven § 224. En annen sak er at kildevernet kan begrense politiets og påtalemyndighetens adgang til å bruke slikt materiale som bevis i en straffesak.

Det er videre klart at de alminnelige begrensningene på politiets og påtalemyndighetens tilgang til data, også vil gjøre et eventuelt inngrep i pressens kildevern mindre. For eksempel vil den tidsmessige begrensningen av lagringsplikten, vilkårene for utlevering av data og domstolenes kontroll med at vilkårene for tilgang opplysningene er oppfylt, medføre at inngrepet avtar i styrke.

Styrken i inngrepene i pressens kildevern vil også variere etter hvordan politiet eller påtalemyndighet begjærer tilgang til data. Vedrørende kontroll av kommunikasjon mellom journalist og kilde, uttaler Metodekontrollutvalget (NOU 2009: 15 kapittel 28.5.2 side 337):

> «Sett i sammenheng, tyder disse avgjørelsene på at kontroll av kommunikasjon med det formål å avsløre identiteten til pressens kilder er å anse som et svært alvorlig inngrep i retten til kildevern. Kjennelsen i Weber og Saraviasaken tyder på at dette også må gjelde kommunikasjonskontroll og annen avlytting rettet mot journalisters virksomhet.

Videre tilsier Weber og Saravia-saken at kontroll av kommunikasjon mellom journalister og kilder som utilsiktet konsekvens av at andre personers telefon er underlagt kontroll utgjør et langt mindre alvorlig inngrep, og at det i utgangspunktet ikke kan kreves at det nasjonale regelverket må inneholde særlige regler til beskyttelse av kilders identitet i slike tilfelle. Avgjørelsen av om inngrepet likevel er uforholdsmessig må antas å bero på en vurdering av om regelverket er egnet til å sikre at inngrepene begrenser seg til det som var nødvendig for å oppnå det aktuelle formålet, og da særlig om vilkårene for inngrepet er tilstrekkelige og effektive med hensyn til å begrense avsløringen av journalisters kilder til et uunngåelig minimum.»

Straffeprosessloven § 170 a knesetter den generelle hensiktsmessighets- og forholdsmessighetsvurderingen som enhver beslutning om bruk av tvangsmidler skal undergis. Metodekontrollutvalget er imidlertid i tvil om hvorvidt denne bestemmelsen gir en tilstrekkelig beskyttelse for kildevernet (NOU 2009: 15 kapittel 28.3 side 334):

«I Rt. 2007 side 1507 tok Høyesteretts kjæremålsutvalg stilling til om en journalist hadde plikt til å utlevere journalistisk materiale som ikke var kildeavslørende. Det var klart at unntaket i § 210 a tredje ledd ikke kom til anvendelse, men det var anført at et pålegg om utlevering rettet mot en journalist var uforholdsmessig etter straffeprosessloven § 170 a. Kjæremålsutvalget kom til at straffeprosessloven § 170 a var uriktig forstått når lagmannsretten mente at utleveringsbegjæringer overfor pressen bare helt unntaksvis kan imøtekommes, og at vektige grunner var påkrevd. Avgjørelsen tyder på at hensynet til medienes rolle i samfunnet ikke er relevant i forholdsmessighetsvurderingen etter § 170 a der det ikke dreier seg om utlevering av kildeavslørende materiale. Den behøver imidlertid ikke innebære at hensynet til pressens kildevern er irrelevant ved vurderingen av om politiet skal få tillatelse til bruk av andre tvangsmidler som vil kunne føre til at en kildes identitet avsløres. Dette spørsmålet synes ikke å ha vært behandlet i høyesterettspraksis.»

Metodekontrollutvalget kommer etter dette med følgende anbefaling (NOU 2009:15 kapittel 28.7 side 339-340):

«Etter utvalgets oppfatning bør hensynet til pressens kildevern, EMDs syn på dette spørsmålet og Europarådets anbefaling kunne ivaretas ved at de gjøres til momenter i vurderingen av om bruk av den aktuelle etterforskingsmetoden vil være forholdsmessig etter straffeprosessloven § 170 a. Videre vil hensynet til kildevernet i stor utstrekning ivaretas av utvalgets forslag om å innføre begrensninger i adgangen til å føre som bevis kildeavslørende opplysninger innhentet gjennom kommunikasjonskontroll og romavlytting, jf. nedenfor. Foretas en slik forholdsmessighetsvurdering, antas en eventuell kontroll av kommunikasjon med hensikt å avdekke en kildes identitet, ikke å komme i konflikt med EMK artikkel 10.»

Hvorvidt utformingen av straffeprosessloven § 170 a ivaretar pressens rett til kildevern er således en mer generell problemstilling som knytter seg all bruk av tvangsmidler. Vurderingen av hvorvidt pressens kildevern bør styrkes ytterligere for eksempel ved endringer i straffeprosessloven § 170 a, vil bli vurdert i forbindelse med oppfølgningen av Metodekontrollutvalgets utredning. Metodekontrollutvalgets utredning har vært ute på høring. Høringen ble avsluttet sommeren 2010 og Justisdepartementet arbeider nå med å følge opp saken.

Datatilsynet og *Rødt* har anført at den foreslåtte gjennomføringen av datalagringsdirektivet også vil kunne krenke forsamlings- og foreningsfriheten. Dette er et en rettighet som blant annet er beskyttet av EMK artikkel 11. Departementet ser at innføring av lagringsplikt kan ha en side til forsamlings- og foreningsfriheten, men legger til grunn at gjennomføringen eventuelt vil medføre et begrenset inngrep i disse frihetene, se for øvrig kapittel 6.4 og vurderingen av nedkjølende effekt. På samme vis som eventuelle inngrep i retten til privatliv, korrespondanse og ytringsfrihet kan rettferdiggjøres etter EMK artikkel 8 nr. 2 og 10 nr. 2, legger departementet til grunn at også eventuelle inngrep i forsamlings- og foreningsfriheten kan rettferdiggjøres etter EMK artikkel 11 nr. 2.

3.3.4 Uskyldspresumsjonen

Vernet etter både EMK artikkel 6 nr. 2 og SP artikkel 14 nr. 2 innebærer at enhver som er siktet for en straffbar handling er uskyldig inntil skyld er bevist etter loven. Datalagringsdirektivet stiller krav om lagring uavhengig av om det foreligger noen mistanke eller siktelse. Den myndighetspålagte lagringsplikten kan således ikke forstås som

uttrykk for noen mistanke eller annen form for beskyldning om at det er begått et straffbart forhold, verken mot befolkningen som sådan, eller mot konkrete personer. Departementet kan derfor vanskelig se at den foreslåtte gjennomføringen av datalagringsdirektivet skulle krenke uskyldspresumsjonen.

3.3.5 Øvrige forpliktelser

SP artikkel 17 og FNs barnekonvensjon artikkel 16 beskytter, som EMK artikkel 8, retten til privatliv og korrespondanse. Bestemmelsene er bygget noe annerledes opp enn EMK artikkel 8, men kravene om at inngrepet må være ulovlig og vilkårlig, vil i prinsippet gi rom for samme form for rettferdiggjøring av et inngrep som under EMK artikkel 8 nr. 2. Også eventuelle inngrep etter bestemmelsene i SP artikkel 19 og FNs barnekonvensjon artikkel 13 og 14 (ytringsfrihet) samt SP artikkel 21 og 22 og FNs barnekonvensjon artikkel 15 (forenings- og forsamlingsfrihet), må kunne rettferdiggjøres på tilsvarende vis som under EMK artikkel 10 og 11.

Av betydning for tolkningen av FNs barnekonvensjon artikkel 16, er det også at barnekonvensjonen artikkel 34 fastsetter at statene må treffe egnede nasjonale, bilaterale og multilaterale tiltak for å hindre seksuell utnytting og seksuelt misbruk av barn, jf. også 5.4.7.4.

Det vil på den annen side ikke være riktig å si at Norge på dette grunnlaget er folkerettslig forpliktet til å gjennomføre datalagringsdirektivet i norsk rett. Materielt sett kan imidlertid bestemmelser om lagring av data være av en slik karakter at de har avgjørende betydning for politiets muligheter til å bekjempe kriminalitet, jf. nærmere redegjørelse i kapittel 5.

4 Implementering av datalagringsdirektivet i Europa

4.1 Danmark

I Danmark er datalagringsdirektivet 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. I disse tilfellene gjelder ikke kravet om at dataene knytter seg til én mistenkt. Opplysninger om lokaliseringen av en mobiltelefon kan innhentes dersom telefonen antas å bli benyttet av en mistenkt, forutsatt at inngrepet antas å være av vesentlig betydning for etterforskningen og denne gjelder et lovbrudd som kan medføre fengsel i 1 år og 6 måneder eller mer (§ 791 a stk. 5).

Når det gjelder abonnements- og brukerdata, følger det av lov nr. 780 af 28. september 2006 om konkurrence og forbrugerforhold på telemarkedet § 15 c at tilbydere av elektroniske kommunikasjonstjenester til sluttbrukere, på begjæring skal utlevere slike opplysninger til politiet. Slik utlevering skjer etter reglene om edisjon (utlevering), jf. retsplejeloven § 804. Pålegg om utlevering av slike opplysninger kan meddeles dersom det er grunn til å anta at opplysningene kan tjene som bevis.

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.

Det danske Finanstilsynet har med hjemmel i § 87 stk. 2, i lov om værdipapirhandel m.v., jf. lovbekendtgørelse nr. 959 af 11. august 2010, rett til å kreve utlevert data direkte fra tilbyderne i den grad det er nødvendig for å utøve tilsynets virksomhet. Bestemmelsen gjennomfører direktiv 2003/6/EF om markedsmisbruk («markedsmisbruksdirektivet») artikkel 12 nr. 2 bokstav d og direktiv 2004/39/EF om markeder for finansielle instrumenter («MiFID») artikkel 50 nr. 2 bokstav d i dansk rett.

4.2 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 loven § 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, og forutsatt at opplysningene kan antas å være av vesentlig betydning for etterforskningen. Overvåkningen kan gjelde «teleanslutning, teleadress eller teleterminalutrustning» som den mistenkte innehar eller kan tenkes å anvende, eller det kan gis tillatelse til innhenting av posisjoneringsdata for mobiltelefon som den mistenkte innehar eller kan tenkes å inneha. Overvåkning av andre enn mistenktes mobil mv. kan skje etter samtykke fra den som overvåkes (5 a kapittel 3 § 2).

5 a kap. 3 a § hjemler i tillegg innhenting av basestasjonsdata uavhengig av om det foreligger mistanke mot en konkret person dersom opplysningen kan antas å være av vesentlig betydning for etterforskningen. Også her gjelder strafferammekravet, alternativt at saken gjelder ovenfor nevnte straffbare handlinger.

Beslutning om tillatelse til teleovervåkning og innhenting av basestasjonsdata treffes av domstolen etter skriftlig begjæring fra tjenestemann med pågripelsesrett, men slik at tjenestemannen har hastekompetanse dersom beslutningen ikke kan utsettes (5 a kap. 5 § 1 og 2).

I tillegg gir lagen om dataskydd vid elektronisk kommunikation 9 kapittel 35 § nødsentralen og politiet rett til å få utlevert identifiserings-, lokaliserings- og abonnements- og brukerdata i forbindelse med nødmeldinger, uavhengig av taushetsplikt.

Politiet har dessuten rett til å få identifiseringsopplysninger for å hindre, avsløre eller etterforske lovbrudd etter reglene i polislagen, jf. lagen om dataskydd vid elektronisk kommunikation 9 kapittel 36 §, jf. polislagen 3 kapittel 36 § 2 mom. Vilkåret er at opplysningene i det enkelte tilfellet er nødvendig for utførelsen av politiets oppgaver. Endelig så har politiet også rett til, på visse vilkår, å få hentet ut identifiseringsopplysninger i forbindelse med brudd på besøksforbud, telefonforstyrrelse, og telefonsjikane (hemfridsbrott).

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).

Finansinspektionen har kompetanse til å føre tilsyn med handel med finansielle instrumenter. Dette organet har imidlertid ikke direkte tilgang til eksisterende trafikkdata i medhold av direktiv 2003/6/EF om markedsmisbruk («markedsmisbruksdirektivet») og direktiv 2004/39/EF om markeder for finansielle instrumenter («MiFID»). Ved implementeringen av direktivene ble en slik direkte tilgang funnet å være uforenlig med den finske Grundlagen 10 § om skydd för privatlivet som lyder «Vars och ens privatliv, heder och hemfrid är tryggade. Närmare bestämmelser om skydd för personuppgifter utfärdas genom lag». Finansinspektionen er således henvist til å søke bistand fra politi og påtalemyndighet når det har behov for tilgang til data i forbindelse med utførelsen av sine tilsynsoppgaver.

4.3 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 EU-domstolen. Domstolen avsa 4. februar 2010 dom mot Sverige på grunn av manglende gjennomføring av datalagringsdirektivet.

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 er nettopp fulgt opp ved lagrådsremiss 11. november 2010. Remissen, som inneholder regjeringens forslag til gjennomføring av datalagringsdirektivet, skal gjennomgås av lagrådet for granskning før det i neste omgang legges frem for Riksdagen. I forslaget som nå foreligger foreslås innført en lovpålagt plikt for tilbydere av offentlig elektronisk

kommunikasjonsnett og –tjenester til å lagre data spesielt for kriminalitetsbekjempelsesformål. Lagringstiden foreslås satt til seks måneder. Etter den tid inntrer en sletteplikt, likevel slik at data som er begjært utlevert innen utløpet av seksmånedersfristen skal lagres inntil de er blitt utlevert. Det legges opp til at tilbyderne skal stå for kostnadene med lagring, sikkerhet og tilpasning av systemer, mens myndighetene som begjærer utlevering skal erstatte leverandørenes kostnader forbundet med utlevering av data. Forslaget følger hovedkategoriene i direktivet for hva som skal lagres. Nærmere bestemmelser om sikring av lagrede data, hvilke data som skal lagres og om leverandørenes rett til erstatning for utlevering av opplysninger skal fastsettes i forskrift. Det legges opp til forhåndsbestemte, standardiserte erstatningsbeløp for utlevering av opplysninger.

I svensk rett er det allerede i dag adgang til å få ut data. Det skilles mellom ulike typer data, tilgang for ulike myndigheter og i ulike situasjoner (i og utenfor etterforskning).

Innhenting av trafikkdata kan for det første skje etter reglene om teleovervåkning i rättegångsbalken 27 kapittel om beslag, hemlig teleövervakning m.m. i. Hemmelig teleovervåkning omfatter blant annet innhenting av teleforsendelser som er sendt til eller fra en bestemt teleadresse. Et grunnleggende vilkår for slik teleovervåkning er at det er mistanke om lovbrudd som har en minstestraff på seks måneders fengsel, eller datakriminalitet, grovere tilfeller av barnepornografi eller narkotikaforbrytelser. Eksempler på straffbare handlinger som har en minstestraff på seks måneders fengsel er drap, menneskehandel, grov tvang, grov fredskrenkelse, grov trussel, grove seksuelle overgrep mot barn, og grov hallikvirksomhet. Det er videre et vilkår at det foreligger skjellig grunn til mistanke mot en person og at innhentingen må antas å være av vesentlig betydningen for etterforskningen. Tillatelse til teleovervåkningen gis av retten etter begjæring fra påtalemyndigheten.

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.

Remissen som ble fremlagt 11. november 2010 legger opp til at opplysninger lagret i henhold til lagringsplikten bare skal kunne utleveres til kriminalitetsbekjempende myndigheter. Men det foreslås ikke endringer i gjeldende regler om adgang til å lagre for andre formål enn kriminalitetsbekjempelse, særlig faktureringsformål. Det gjøres heller ikke endringer i reglene for utlevering av opplysninger lagret for slike andre formål til andre enn kriminalitetsbekjempende myndigheter, for eksempel skattemyndigheter.

I Polismetodutredningen, SOU 2009: 1 En mer rättssäker inhämtning av elektronisk kommunikation i brottsbekämpningen foreslås at politiets tilgang til data skal reguleres av rättegångsbalkens regler om hemmelig teleovervåkning. I tillegg foreslås en egen, ny lov om tilgang for etterretningsformål.

For abonnementsopplysninger foreslås straferammekravet lempet slik at det skal være tilstrekkelig at forholdet kan straffes med bot. Denne reguleringen fremgår fortsatt av lagen om elektronisk kommunikation.

I rättegångsbalken opprettholdes kravet om at det må foreligge mistanke mot en bestemt person. Utlevering skal imidlertid også kunne skje i andre tilfeller dersom opplysningene er av vesentlig betydning for etterforskningen og formålet enten er å etablere mistanke eller er av vesentlig betydning på annen måte. Strafferammekravet om minstestraff på seks måneders fengsel, i tillegg til at enkelte handlinger er særskilt oppregnet, videreføres. Men dersom det ikke ennå foreligger mistanke mot noen, kreves det at den aktuelle handlingen har et straffnivå på minst to års fengsel.

Utlevering til etterforskningsformål skal som hovedregel besluttes av retten, men slik at mindre omfattende eller lite inngripende teleovervåkning skal kunne besluttes av politi og påtalemyndighet når det ennå ikke foreligger mistanke mot en bestemt person. Videre foreslås innført hastekompetanse for påtalemyndigheten. Det skal som hovedregel underrettes om hemmelig teleovervåkning unntatt hvor etterforskningen gjelder særskilt oppregnede handlinger. Underretning er heller ikke nødvendig etter basestasjonssøk eller dersom utleveringen antas å være lite inngripende.

En remiss som følger opp Polismetodutredningen er varslet fremlagt for lagrådet for granskning om kort tid.

Finansinspektionen fører tilsyn med verdipapirmarkedet i Sverige. Den har som ledd i sin virksomhet rett til å anmode et finansforetak om utlevering av data, jf. lag (1991: 980) om handel med finansiella instrument 6 kap. 1 a § første ledd

nr. 1 og lag (2005: 377) om straff för marknadsmissbruk vid handel med finansiella instrument 16 § annet ledd. Bestemmelsene gjennomfører markedsmisbruksdirektivet artikkel 12 nr. 2 bokstav d i svensk rett. Rett til å anmode om utlevering av data følger også av lag (2007: 528) om värdepappersmarknaden 23 kap. 2 § samt 13 kap. 7 § annet ledd som gjennomfører MiFID artikkel 50 nr. 2 bokstav d.

Bestemmelsene gir neppe Finansinspektionen adgang til å begjære utlevering av data fra tilbyderne. Finansinspektionen i Sverige har imidlertid en noe annen rolle enn det norske Finanstilsynet, i den forstand at Finansinspektionen selv ikke gjør noen undersøkelser ved mistanke om brudd på adferdsbestemmelsene i verdpapirhandellovgivningen, men oversender enhver mistanke til politiet (Ekobrottsmyndigheten) på svært lav terskel. Det er derfor i praksis alltid politiet i Sverige som tar beslutning om eventuelt å innhente trafikkdata dersom dette er relevant bevismateriale i den aktuelle saken.

4.4 Andre EU-land

Alle EUs medlemsstater har gjennomført datalagringsdirektivet i nasjonal lovgivning med unntak av Sverige, Irland, Hellas og Østerrike. EUs medlemsstater har innført ulik lagringstid. Den gjennomsnittlige lagringstiden i land som har gjennomført direktivet er 12 måneder. I de fleste statene er det nødvendig med en tillatelse fra retten for å få utlevert data.

EU-kommisjonen har gått til sak mot Hellas, Østerrike, Irland, Polen og Nederland i tillegg til Sverige 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 man har fått opplyst fra greske myndigheter, er treghet i statsadministrasjonen den viktigste årsaken til forsinkelsen.

Det har vært reist spørsmål ved gjennomføringen av direktivet i nasjonal rett i Romania, Tyskland og Ungarn. Den rumenske konstitusjonsdomstolen avsa 8. oktober 2009 en dom hvor den la til grunn at den rumenske loven som gjennomfører datalagringsdirektivet, er i strid med 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 i strid med den rumenske grunnlovens bestemmelser om retten til respekten for privatliv.

Avgjørelsen i den tyske forfatningsdomstolen i Karlsruhe

Den tyske forfatningsdomstolen (første senat) fant i dom 2. februar 2010, i sakene 1 BvR 256/08, 1 BvR 263/08 og 1 BvR 586/08, at den tyske føderale lovgivningen som skulle gjennomføre datalagringsdirektivet var i strid med den tyske forfatningen artikkel 10. Gjennomføringsloven ble vedtatt høsten 2007 og trådte i kraft 1. januar 2008. Avgjørelsen ble avsagt under dissens 6-2. Både flertallet og mindretallet la til grunn at gjennomføringen av datalagringsdirektivet har et legitimt formål, og at formålet med lagringen vanskelig kan oppnås med andre, mildere midler, jf. dommen avsnitt 207 og 208. En enstemmig forfatningsdomstol kom således til at en myndighetspålagt lagringsplikt av trafikkdata i 6 måneder, slik som foreskrevet i datalagringsdirektivet, i seg selv ikke strider mot forfatningen artikkel 10. Lagringsplikten vil imidlertid bare være i samsvar med forfatningen artikkel 10 dersom utformingen av regelverket om lagring og bruk av trafikkdataene tilfredsstiller de nærmere kravene til forholdsmessighet som følger av forfatningen artikkel 10, jf. dommen avsnitt 219. I den nærmere vurderingen av den tyske gjennomføringslovens forholdsmessighet, målt opp mot den tyske forfatningen artikkel 10, delte forfatningsdomstolen seg i et flertall på seks dommere og et mindretall på to dommere. Flertallet fant at hele den føderale gjennomføringsloven ikke tilfredsstilte kravene til forholdsmessighet som følger av forfatningen artikkel 10. Et mindretall på én dommer fant at hele den føderale gjennomføringsloven tilfredsstilte kravene til forholdsmessighet, mens et mindretall på én dommer fant at deler av den føderale gjennomføringsloven ikke var i samsvar med forfatningen artikkel 10.

Flertallet fremhevet at gjennomføringsloven var uforholdsmessig av en rekke grunner. Det ble blant annet pekt på at gjennomføringsloven ikke sikret tilstrekkelig beskyttelse av lagret informasjon, jf. dommen avsnitt 221 til 225 og 271 til 275, eller inneholdt tilstrekkelige begrensninger på tilgang og bruk av lagret informasjon, jf. dommen avsnitt 226 til 238, 276 til 279 og 285 til 286. Det ble også pekt på at grunnreglen må være at individer det hentes ut informasjon om, skal informeres om at dette gjøres, jf. dommen avsnitt 240 til 245 og 280.

5 Behovet for data i kriminalitetsbekjempelsen

5.1 Innledning

I høringsnotatet kapittel 4.3 omtalte departementene den teknologiske utviklingen, hvor nye kriminalitetsformer har oppstått. Den «nye» kriminaliteten muliggjøres av ny teknologi, og dette utfordrer politiet. Utviklingen har gitt de kriminelle nye muligheter til å utføre lovbrudd og unndra seg kontroll og straffeforfølgning.

Erkjennelsen av behovet for data som et svært viktig og brukbart redskap i forebygging, etterforskning, avsløring og straffeforfølgning av kriminalitet, spesielt organisert kriminalitet, fremgår av datalagringsdirektivets fortale nr. 7, 9, 10 og 11. Norsk politi har innhentet og brukt elektroniske data fra tilbyderne fra den tid mobiltelefonen fikk sin utbredelse. Ranet av maleriet «Skrik» fra Nasjonalgalleriet i 1994 er det eldste sakseksemplet det er vist til i dette kapittelet (5.4.7.7). Det er en utbredt oppfatning hos politi og påtalemyndighet at elektroniske data har nytteverdi i kriminalitetsbekjempelsen. Elektroniske data veier normalt tungt som bevis, siden de er objektiv konstaterbare. Slike bevis bidrar til å rekonstruere et hendelsesforløp gjennom å se på hvilket kommunikasjonsmønster eller bevegelsesmønster mistenkte har. Elektroniske data kan ha stor betydning som innledende bevis, ved at de kan identifisere mistenkte og gi grunnlag for annen bevissikring, som innhenting av DNA-prøve, ransaking og avhør.

Nytten av elektroniske data som bevis kommer ikke nødvendigvis til syne i domsgrunnene. Mistenktes visshet om at politiet har hentet ut elektroniske data, eller motstrid som påvises mellom mistenktes første forklaring og uthentede data, kan bane veien for at han avgir en *ny* forklaring som senere utgjør hovedbeviset i saken. Blir siktede først under tingrettsbehandlingen konfrontert med motstrid med fremlagte elektroniske data, kan nytten av slike data bli sentral i rettens bevisvurdering. Ankes dommen inn for en høyere instans, hender det ofte at ankeinstansen legger til grunn underinstansens bevisvurdering som ubestridt av partene. Etterforskningens forløp er normalt ikke gjenstand for oppmerksomhet under hovedforhandlingen, og blir derfor lite omtalt i straffedommen.

Nytteverdien av elektroniske data ble ikke særskilt undersøkt i Metodekontrollutvalgets utredning NOU 2009:15 «Skjult informasjon – åpen kontroll», men utvalget viste til at slike data har vært til nytte i omtrent 40 % av sakene hvor data ble innhentet (utredningen s. 116). Utvalget støttet seg til en tysk undersøkelse fra 2008 (Albrecht/Grafe/Kilching). Metodekontrollutvalget uttalte (s. 122):

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

En rekke saker viser at politidistriktene har kommet til kort fordi de ikke i tilstrekkelig grad har lyktes i å samarbeide og dele informasjon med andre politidistrikter i saker som gjelder omreisende kriminelle. På samme måte vil bekjempelsen av grenseoverskridende organisert kriminalitet og terror komme til kort dersom det internasjonale politi- og påtalesamarbeidet ikke prioriteres. Datalagringsdirektivet er i seg selv et uttrykk for en samordnet europeisk innsats mot alvorlig kriminalitet. I bekjempelsen av alvorlig kriminalitet i Europa forutsettes det at norsk politi er i stand til å bidra med nødvendige data til våre samarbeidspartnere. Uavhengig av eventuell implementering av datalagringsdirektivet mener politiet at det uansett må gjennomføres lovendringer for å sikre nødvendig lagring av data.

Til forskjell fra straffeloven 1902, har straffeloven 2005 et eget kapittel (kapittel 21) om vern av informasjon og informasjonsutveksling. Dette gjenspeiler informasjonsrevolusjonen som har funnet sted, og har i seg selv direkte betydning for behovet for elektroniske data i kriminalitetsbekjempelsen. Tilblivelsen av nye straffebud og revisjonen av eksisterende straffebud som gjelder datakriminalitet eller kriminalitet hvor informa-

sjonsteknologi benyttes, skaper nye behov for politiets tilgang til data. Politidirektoratets beskrivelse av utviklingen er treffende:

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

5.2 Høringsnotatets forslag

Departementene omtalte behovet for lagrede data i kapittel 4.1 i høringsnotatet (s. 23-24). Politiet skal «gjennom forebyggende, håndhevende og hjelpende virksomhet være et ledd i samfunnets innsats for å fremme og befeste borgernes rettssikkerhet, trygghet og alminnelige velferd for øvrig», jf. politiloven § 1. I mange tilfeller er tilgangen til data helt avgjørende for at politiet skal kunne ivareta de oppgaver som etaten er tillagt etter politiloven. Gjennom politiets innsats skal borgernes behov for rettssikkerhet, trygghet og alminnelig velferd sikres, og etaten er derfor tillagt metoder og virkemidler for å ivareta disse oppgavene. Ny teknologi gir de kriminelle nye muligheter til å kommunisere med hverandre i planleggingen av straffbare handlinger, og øker farene for internasjonal organisering av forbrytelsene. Trafikkdata, lokaliseringsdata og abonnementsdata vil være viktige for politi og påtalemyndighet som bevis i straffesakene, og i enkelte saker er slike data avgjørende bevis, eksempelvis ved ulovlig nedlasting av barnepornografi fra Internett.

Fra fornærmedes ståsted er sikring av tilgangen til data viktig, slik at krenkelse begått av andre borgere kan bekjempes effektivt. Samfunnets interesse vil være at saken avgjøres på et materielt riktig grunnlag. Innhentede data kan også godtgjøre omstendigheter som medfører at et påstått straffbart forhold ikke kan legges til grunn som tilstrekkelig bevist. I alminnelighet vil bedre opplysning av straffesakene medføre at antallet uriktige domfellelser reduseres. Tilgang til data er også viktig ved forebygging av alvorlig kriminalitet og terrorhandlinger. I enkelte straffesaker kan det oppstå behov for innhenting av data når det har gått en del tid, for eksempel under pådømmelse i lagmannsrett. Korte slettefrister kan da være et problem, uansett om det er påtalemyndigheten, tiltalte ved sin forsvarer eller retten i medhold av straffeprosessloven § 294, som tar initiativet til innhenting av lagrede data. Betydningen av data ble også beskrevet i høringsnotatet kapittel 4.8 om lagringstid (s. 39-41). Enkelte alternativer til historiske data, herunder sikringspålegg jf. straffeprosessloven § 215 a og kommunikasjonskontroll etter straffeprosessloven kapittel 16 ble omtalt i høringsnotatet kapittel 2.4.

5.3 Høringsinstansenes syn

Utenriksdepartementet, Riksadvokaten, Det nasjonale statsadvokatembetet, Oslo statsadvokatembeter, Politiets sikkerhetstjeneste, Politidirektoratet, Økokrim, Kripos, Datatilsynet, Post- og Teletilsynet, Institutt for informatikk ved Universitetet i Oslo, Barneombudet, Telenor, NetCom, Ventelo, Politijuristene, Politiets fellesforbund, Juristforbundet PRIVAT, Hovedorganisasjonen for handel og tjenester HSH, UNIO, Næringslivets sikkerhetsråd, Norsk narkotikapolitiforening, TEKNA, NITO, IKT Norge, Redd barna, FriBit, EL&IT Forbundet, Stiftelsen Elektronikkforbundet, Norsk forening for kriminalreform (KROM), Elektronisk forpost Norge og *Nei til EU Hordaland* har uttalt seg om behovet for data i kriminalitetsbekjempelsen.

5.3.1 Høringsinstansene – generelt om behovet for datalagringsdirektivet

Riksadvokaten mener debatten om implementering *mer* er et spørsmål om hva man mister enn å innføre noe nytt; adekvate alternativer finnes ikke. Riksadvokaten sier videre at «utsatt sletting» vil kunne ha vekt i favør av siktede og som bevis for uskyld. Embetet advarer mot å etablere ordninger som svekker politiets evne til å oppklare straffbare forhold. Lagres ikke data, vil kriminelle fritt kunne kommunisere uten fare for at myndighetene i ettertid kan spore kontakten.

Det nasjonale statsadvokatembetet uttaler at datalagringsdirektivet er

> «avgjørende for fremover å kunne motvirke organisert kriminalitet og terror på en effektiv måte. Det er ikke mulig å være for en effektiv bekjempelse av terror og organisert kriminalitet (selv kun med moderate virkemidler) og samtidig være mot gjennomføringen av datalagringsdirektivet. Å være for bekjempelse av organisert kriminalitet og samtidig mot implementering av datalagringsdirektivet er i realiteten en selvmotsigelse. Å ikke gjennomføre datalagringsdirektivet vil innebære en merkbar reell nedprioritering av kampen mot organisert og annen alvorlig kriminalitet … Så vidt vites er det ingen samfunn noen gang som har hatt en situasjon hvor ikke historiske spor fra mobil og internettbruk er sporbare».

Oslo statsadvokatembeter uttaler at det «selvsagt» er rimelig å anta at økt datamasse som lagres i lang tid i prinsippet vil være nyttig for politiets etterforskningsarbeid, men at nytteverdien er betinget av flere forhold. Det er vanskelig å ha bastante oppfatninger av den konkrete nytteverdien uten å gjennomgå den enkelte sak. Trafikkdata vil kunne gi nyttig informasjon om hvordan etterforskningen skal innrettes. Det vil være nyttig å øke det potensielle informasjonstilfang i kriminalitetsbekjempelsen, men det er vanskelig å ha sikre oppfatninger ut over en generell antagelse.

Økokrim uttaler at trafikkdata gir vesentlige og tidvis avgjørende bidrag til etterforskningen og pådømmelsen av alvorlige økonomiske og miljørelaterte straffesaker. *Politidirektoratet* uttaler at manglende lagring av trafikkdata vil innebære noe nytt i norsk kriminaletterforskning. Manglende lagring innebærer at åsted, verktøy og spor i forbindelse med kriminelle handlinger utslettes. Ved et seksuelt overgrep foretatt via et web-kamera utgjør selve kommunikasjonen det objektive beviset for forbrytelsen: «Uten lagring vil beviset for overgrepet kun være tilgjengelig i barnets traume og i gjerningsmannens sinn». *Politidirektoratet* viser til Grunnloven § 102, som setter forbud mot husinkvisisjoner med unntak for kriminelle tilfeller, men hvor politiet etter bestemte prosedyrer – ofte under domstolens kontroll – gis adgang til å foreta inngrep. Dersom elektroniske data ikke lenger lagres, gjør man i realiteten Internett til et «hus» som politiet ikke har tilgang til, selv om det er mistanke om alvorlige kriminelle handlinger.

Kripos uttaler at elektroniske data er et av de helt avgjørende basisverktøyene i politiets «verktøykasse». Det er et verktøy som hver eneste dag bidrar vesentlig til oppklaring av alvorlige forbrytelser. Ingen andre metoder gir den samme type informasjon og det finnes ikke noe alternativ til trafikkdata i politiets «verktøykasse».

Post- og teletilsynet slutter seg til at data benyttes i et ikke ubetydelig omfang og at politiet anser dette som en effektiv etterforskningsmetode. *Barneombudet* uttaler at manglende bekjempelse av kriminalitet hvor barn er ofre, synes å skyldes andre grunner enn fraværet av datalagringsdirektivet. *Politijuristene* er grunnleggende positive til norsk implementering av datalagringsdirektivet, og uttaler at konsekvensene av manglende innføring vil bli negative, merkbare og vil øke over tid. *Juristforbundet PRIVAT* uttaler at direktivet vil kunne forhindre visse typer planlagt aktivitet, men det er tvilsomt om det vil forhindre impulsive fysiske overgrep. Datalagring vil kunne oppklare noen slike forbrytelser, men de som planlegger terror vil ha ressurser til å kommunisere på måter som gjør at oppklaring likevel blir vanskelig.

HSH oppfatter at datalagringsdirektivet er viktig for politiets kriminalitetsbekjempelse, og viser til at medlemmene i HSH de senere år har opplevd en stor økning i vinningskriminaliteten. *Næringslivets sikkerhetsråd* uttaler at politi- og påtalemyndighet må ha metoder og muligheter til å oppklare alvorlige straffesaker som står i forhold til kriminalitets- og teknologiutviklingen. *TEKNA* uttaler at de enorme muligheter til bruk og misbruk som de nye kommunikasjonsformene medfører, kan tilsi lagring slik at myndigheten kan gripe inn dersom ulovligheter begås. *NITO* uttaler at det ikke er godt nok utredet hvorfor innføringen av datalagringsdirektivet er nødvendig for å bekjempe kriminalitet. *EL&IT Forbundet* uttaler at det ikke synes dokumentert i høringsnotatet at datalagring er nødvendig for kriminalitetsbekjempelsen. *Stiftelsen Elektronikkforbundet* og *Norsk forening for kriminalreform (KROM)* uttaler at politiet i dag har de nødvendige hjemler for å få tilgang til den informasjon de ønsker. *Nei til EU Hordaland* uttaler at det er manglende teknisk og mannskapsmessig kapasitet som begrenser politiets arbeidsmuligheter, og ikke manglende tilgang til trafikkdata.

Flere høringsinstanser viser til tidligere offentlige utredninger og publikasjoner hvor behovet for datalagring er omtalt. I kapittel 5.4.2 omtales disse i kronologisk rekkefølge.

5.3.2 Høringsinstansene om internasjonale forpliktelser og internasjonalt politi- og påtalesamarbeid

Utenriksdepartementet viser til at sammenhengen mellom informasjonsteknologi og terrorisme og annen alvorlig kriminalitet er understreket i en rekke internasjonale fora, og at tilgang til trafikkdata kan ha betydning for effektiviteten av det justispolitiske samarbeidet mellom politi- og påtalemyndigheter. Noen av anbefalingene det er vist til gjengis under 5.4.3. Utenriksdepartementet understreker også betydningen av det internasjonale politisamarbeidet. *Riksadvokaten* uttaler at internasjonalt politisamarbeid kan bli vanskeliggjort uten implementering av direktivet. *Det nasjonale statsadvokatembetet og Kripos* uttaler at datalagring er et målrettet tiltak som på egnet måte sikrer at Norge oppfyller internasjonale forpliktelser og menneskerettslige forpliktelser til å ha en rimelig og effektiv rettshåndhevelse overfor alvorlig kriminalitet. Manglende lagring av abonnementsdata på IP-adresser ut over tre uker er neppe forenlig med Norges internasjonale forpliktelser. Manglende tilgang til elektroniske data skaper vanskeligheter for norske politimyndigheter i det internasjonale politisamarbeidet, og konsekvensene kan bli at Norge blir mindre attraktive å samarbeide med i slike saker. Særlig uttalt er manglende lagring av abonnementsopplysninger om IP-adresser som er eldre enn tre uker. Kripos har vist til saker hvor de har mottatt IP-adresser fra samarbeidende politi, men hvor manglende lagring hos tilbyder har medført at man ikke har kunnet identifisere slike data (se avsnittet «Internettdata» i kap. 5.4.6.4).

Politiets sikkerhetstjeneste uttaler at det internasjonale politi- og sikkerhetsarbeidet er helt «avgjørende» i deres virksomhet, og at dette kan bli sterkt skadelidende uten implementering av direktivet. *Kripos* og *Politiets fellesforbund* uttaler at manglende tilgang til nødvendige data i saker som involverer barn i realiteten representerer brudd på FNs barnekonvensjon. *Politiets sikkerhetstjeneste* og *Kripos* frykter at Norge kan bli et «fristed» for kriminalitet som etterlater seg elektroniske spor. *Institutt for rettsinformatikk* (Universitetet i Oslo) og *NITO* avviser dette. *Politiets fellesforbund* og *UNIO* uttaler at internasjonalt politisamarbeid er tid- og ressurskrevende, og at manglende implementering kan sette det internasjonale politisamarbeidet på prøve. *Barneombudet* uttaler at internasjonale tiltak er nødvendige i bekjempelsen av krenkelser av barn. *HSH* uttaler at «særnorske» løsninger bør unngås av hensyn til det internasjonale politisamarbeidet. *NorSIS* uttaler at det er viktig å tilstrebe like krav til lagringstid, sikring, osv. som de land som vi er nært knyttet til i forhold til utveksling av data. *Narkotikapolitiforeningen* viser til Norges generelle forpliktelser til å bekjempe narkotikakriminalitet, slik dette fremgår av FNs konvensjon om ulovlig håndtering av og handel med narkotika og psykotrope stoffer av 1988. *Elektronisk Forpost Norge* uttaler at mange borgere i Europa vil føle seg ukomfortable med at opplysninger om deres liv skal kunne utleveres til politiet i stater der maktapparatet i verste fall er influert av kriminelle, og at slike stater finnes i Europa.

5.3.3 Høringsinstansene om alternativer til bruk av historiske data

Riksadvokaten, Det nasjonale statsadvokatembetet, Politidirektoratet, Kripos, Politijuristene og *Norsk narkotikapolitiforening* har uttalt seg om bruken av kommunikasjonskontroll og sikringspålegg som alternativer til bruk av historiske data. *Det nasjonale statsadvokatembetet* uttaler at det ikke finnes alternative metoder som er mindre inngripende for å oppnå det samme. *Kripos* uttaler at politiets bruk av trafikkdata i etterforskningen ikke kan erstattes av andre eksisterende metoder. *Datatilsynet* uttaler at kommunikasjonskontroll – i motsetning til datalagring – er en målrettet metode som tas i bruk overfor en begrenset krets når det foreligger kvalifisert mistanke. Tilsynet etterspør en belysning av alternative tiltak når datalagring vurderes som nødvendig. *Telenor, IKT Norge, Stopp datalagringsdirektivet* og *Samfunnsorganisasjonen Demos* etterspør en nærmere belysning av alternativene til datalagring. *Redd Barna* uttaler at de savner en vurdering av alternative måter å sikre gode vilkår for etterforskning av saker som gjelder overgrep og krenkelser mot barn, uavhengig av datalagringsdirektivet.

5.3.4 Høringsinstansene om omgåelse av datalagringsdirektivet

Riksadvokaten uttaler at en rekke personer som begår alvorlig kriminalitet, benytter kommunikasjon som faller under lagringsplikten, og at omgåelsesmomentet ikke kan vektlegges ved en vurdering av dagens situasjon. *Kripos* uttaler at spørsmålet om datalagring vil medføre at kriminelle omgår dette, ikke på noen måte er et argument mot å innføre direktivet. Da fingeravtrykksundersøkelser fikk sitt gjennombrudd på begynnelsen av 1900-tallet, ble det hevdet at kriminelle

ville bruke hanser. Men fortsatt oppklares et stort antall saker ved fingeravtrykksundersøkelser. *Politijuristene* uttaler at mye alvorlig kriminalitet begås i affekt. *Telenor* uttaler at en innføring av direktivet åpner for så mange smutthull at det er betimelig å stille spørsmålstegn ved hvor effektivt et slikt tiltak vil være for forebygging og bekjempelse av den typen organisert kriminalitet som er formålet for lagringsplikten. *NetCom* uttaler at det er lett å anta at profesjonelle kriminelle benytter seg av tjenester som ikke har lagringsplikt, og vet hvordan de skal unngå registrering. *NITO* peker på at det har vært en voldsom vridning fra tradisjonell talekommunikasjon over på nettbaserte sosiale medier. *Datatilsynet, Telenor, NetCom, NTNU, Kabel Norge, IKT Norge, Arbeids- og velferdsdirektoratet, Ventelo, Universitetet i Bergen, Elektronisk Forpost Norge, Stopp datalagringsdirektivet, Nei til EU Hordaland* og *Troms, YS, NITO* og *NorSIS* uttaler at det finnes flere måter å omgå datalagringsdirektivet, slik at kriminelle kan kommunisere via kanaler som ikke faller under lagringsplikten etter direktivet. *Oslo statsadvokatembeter, Datatilsynet, IKT Norge, Ifi (Universitetet i Oslo), Stopp datalagringsdirektivet, Telenor, NetCom, Juristforbundet PRIVAT, Universitetet i Troms* og *Raudt Høyanger* omtaler generelt og konkret ulike metoder å omgå datalagringsdirektivet.

5.3.5 Høringsinstansene om behovet for data og ulike typer datas betydning

Datatilsynet vurderer at departementene ikke har foretatt en tilfredsstillende utredning av nødvendigheten, og derfor har tilsynet tatt initiativ til et eget utredningsarbeid for å belyse nødvendigheten. Utredningen ble gjennomført av siv.ing. ph.d. Svein Y. Willassen («Willassen»). Tilsynet uttaler at det er tilbydernes formål som har vært styrende for at slettefristen for IP-adresser etter vedtak er satt til tre uker og at politimessige behov er irrelevante etter hensynene i personopplysningsloven. Tilsynet finner det imidlertid «nokså klart at opplysninger om hvilke personer som er knyttet til ulike IP-adresser vil kunne ha avgjørende betydning når politiet skal etterforske spredning av barneporno». Tilsynet uttaler at henvisningen til at lagrede data kan være nyttig for å sjekke mistenkte ut av saker som etterforskes, rokker ved uskyldspresumsjonen. Departementene skrev i høringsnotatet at innhenting og bruk av trafikkdata mv. vil kunne redusere antallet uriktige domfellelser. *Det nasjonale statsadvokatembetet* uttaler:

> «For dårlig opplysning av faktum kan medføre at politiet griper feil og vi risikerer at uskyldige blir siktet og i spesielle tilfeller domfelt. Trafikkdata motvirker dette. Uskyldige som kommer i politiets søkelys i en etterforsking kan bli sjekket ut av saken fordi trafikkdata viser at deres forklaring om at de hadde alibi for gjerningstidspunktet med all sannsynlighet er riktig. Ved fastsetting av for eksempel drapstidspunkt vil innhenting av data fra offerets mobiltelefon være et viktig bidrag. I den andre Fritz Moen saken var et av de avgjørende spørsmålene om avdøde ble drept natt til lørdag (siste sikre observasjon hvor Fritz Moen hadde alibi) eller minst et døgn senere. I dag ville trafikkdata fra avdødes mobil kunne gitt viktige bevis rundt dette».

Willassen tar utgangspunkt i at en vurdering av nytten vil kunne slå ulikt ut for hver av de typer data som er omhandlet i direktivet, som følge av at dataene er relatert til forskjellige kommunikasjonsformer. Det er derfor av interesse å foreta en slik vurdering og sammenligning for hver kommunikasjonsform, hver for seg. Under kapittel 5.4.6.4 redegjøres det for de viktigste funn i utredningen.

Kripos viser til en tysk undersøkelse (Albrecht/Grafe/Kilchling 2008) omtalt i NOU 2009:15 (Metodekontrollutvalget, s. 122) som viser at «trafikkdata» har vært til nytte i ca. 40 % av sakene i saksutvalget, men Kripos vurderer at nytteverdien av elektroniske data i etterforskning i Norge er langt høyere enn det nevnte undersøkelse viser. Dette var bakgrunnen for at Kripos besluttet å gjennomføre en spørreundersøkelse i mars 2010, om politiets bruk av historiske trafikkdata. Under kapittel 5.4.6.3 redegjøres det for funnene i Kripos' undersøkelse. Også *Økokrim* viser til den tyske undersøkelsen i NOU 2009:15, samt til en svensk undersøkelse omtalt i samme utredning, som viste at bruk av trafikkdata hadde betydning i henholdsvis 47, 50 og 51 % av sakene hvor metoden ble brukt. *Kripos* uttaler at det mangler verifiseringsrutiner ved etablering av epostkonti hos enkelte tilbydere, og at enkelte «anonyme» epostkonti kan sammenlignes med uregistrerte kontantkort. Et skille mellom internettbaserte tilbydere av e-posttjenester og bredbåndstilbydere som samtidig tilbyr e-posttjeneste, er basert på teknologi og bryter med direktivets intensjoner. De data som skal lagres for internettaksess vil dekke politiets behov for å identifisere abonnement til en IP-adresse på et gitt tidspunkt, noe som er det primære behov i dag. *Finanstil-*

synet uttaler at dersom institusjoner og virksomheter utkontrakterer e-postsystemet til en offentlig tilbyder, kan dette medføre lagringsplikt for slike «interne» e-poster. Når det gjelder omfanget av bruk av elektroniske data til nå, har *Kripos* og *Willassen* oppgitt enkelte tall som er innhentet. *NITO* er uenig i at en «utvidet lagringsplikt» vil medføre færre uriktige domsavgjørelser.

5.3.6 Høringsinstansene om saksområder og sakseksempler

Riksadvokaten uttaler at behovet for elektroniske data er et viktig spørsmål, og mener *Politidirektoratet, Kripos* og *PST* har dokumentert dette på en god og overbevisende måte. Riksadvokaten uttaler at det vanskelig kan belegges at manglende tilgang til aktuelt datamateriale vil gi økt kriminalitet i Norge, en slik prognose blir for usikker. Men begått kriminalitet blir vesentlig vanskeligere å oppklare; det er ingen usikkerhet forbundet med denne konklusjonen. *Politiets sikkerhetstjeneste* og *Det nasjonale statsadvokatembetet* uttaler at elektroniske data har avgjørende betydning i det forebyggende arbeidet ved at slike data gir informasjon om kontaktnett, hyppigheten av kontaktene, bevegelsesmønstre og avvik fra et vanlig kommunikasjons- eller bevegelsesmønster. De uttaler at Norge kan bli et «fristed» for terror dersom implementeringen av direktivet ikke gjennomføres. De mener videre at tilgang til elektroniske data er nødvendig, og i mange tilfeller avgjørende, for å kunne ivareta de oppgaver som PST har etter politiloven.

Økokrim uttaler at behovet for trafikkdata er spesielt stort i saker hvor kommunikasjon står sentralt i lovbruddet, for eksempel i saker om verdipapirkriminalitet, kartellvirksomhet, brudd på konkurranselovgivning og saker om korrupsjon. *Politidirektoratet* og *Kripos* har bidratt med en rekke konkrete sakseksempler hvor elektroniske data har blitt benyttet og vært nødvendig for etterforskning og bevisvurdering i retten. Også andre høringsinstanser fra politi og påtalemyndighet har inngitt sakseksempler, og omtalt behovet for ulike typer data på de forskjellige kriminalitetskategorier.

5.4 Tematisk sammenstilling av områder behandlet i høringsuttalelsene

5.4.1 Innledning

Mange høringsinstanser har kommet med sakseksempler og andre innspill knyttet til bruk og behov for data. I det følgende redegjøres det for behovet for data til kriminalitetsbekjempelse oppstilt tematisk. Her inngår også høringsinstansenes innspill på de ulike tema.

5.4.2 Nærmere om offentlige utredninger m.v.

I 2000 avga Sårbarhetsutvalget sin utredning NOU 2000:24 «Et sårbart samfunn» («Willoch-utvalget»). I kapittel 6 «Beskyttelse av IKT og kraftforsyning» anbefalte utvalget enstemmig i pkt. 6.6:

> «For å få til en mer effektiv kriminalitetsbekjempelse ser utvalget behov for følgende tiltak:
> – Tjenestetilbyderne pålegges å føre logger for en begrenset tidsperiode.
> – Dersom politiet retter anmodning forlenges oppbevaringstiden av loggene.
> – Hver sak behandles som enkelttilfelle for å redusere de dilemmaer som hensynet til personvernet gir. Forlenget oppbevaringstid er spesielt aktuelt i påvente av formell begjæring fra utenlandsk politi.
> – Norske myndigheter bør arbeide aktivt for at oppkoblingsinformasjon kan innhentes og utveksles effektivt mellom ulike lands politi.
>
> Utvalget ser behov for å vurdere om det bør innføres plikt for tjenestetilbyderne å rapportere om kjent misbruk av deres tjenester til politiet. Dette er blant annet aktuelt i saker om hvitvasking av penger»

Den 3. november 2003 avga Datakrimutvalget sin delutredning I, NOU 2003: 27 «Lovtiltak mot datakriminalitet». Med grunnlag i Norges forpliktelser etter Europarådets konvensjon om datakriminalitet av 23. november 2001 (Cybercrime-konvensjonen), foreslo utvalget vedtakelsen av en bestemmelse i straffeprosessloven om sikringspålegg, § 215 a. Bestemmelsen ble tilføyd ved lov av 8. april 2005 nr. 16.

Den 29. mars 2004 avga Politimetodeutvalget sin utredning NOU 2004:6 «Mellom effektivitet og personvern. Politimetoder i forebyggende øyemed». Utvalget delte seg i synet på en lagringsplikt (kapittel 10.7.12):

> «Flertallet vil ut fra dette foreslå at det innføres plikt for teleselskapene til å oppbevare trafikk- og posisjonsdata i 1 år slik at politiet får tilgang på viktig informasjon i kriminalitetsbekjempelsen. Selv om det er enorme mengder med per-

sonopplysninger som vil bli lagret, vil det være en mikroskopisk andel av opplysningene som blir utlevert. Og når personvernet er beskyttet gjennom utleveringsbetingelsene, må prinsippet om at personopplysninger bare kan lagres av hensyn til brukerne, vike for hensynet til kriminalitetsbekjempelsen

(…)

Mindretallet ønsker ikke å lovregulere lagringstid. Flertallets forslag medfører at trafikkdata og posisjonsdata om alle telefoner – også personer som ikke kan mistenkes for noe straffbart – vil bli lagret. Ettersom formålet med lagring av trafikk- og posisjonsdata var å dekke tjenestetilbydernes behov for korrekt faktureringsgrunnlag, har politiets bruk vært en form for overskuddsinformasjon – noe som reiser grunnleggende personvernspørsmål … Mindretallet mener det er god grunn til å overlate spørsmålet til Datakrimutvalget».

Den 12. februar 2007 avga Datakrimutvalget sin delutredning II, NOU 2007:2 «Lovtiltak mot datakriminalitet». Utvalget uttalte seg ikke hvorvidt det burde innføres noen plikt for tilbydere å lagre data. EUs datalagringsdirektiv hadde da blitt vedtatt året før (15. mars 2006).

Metodekontrollutvalget avga sin utredning NOU 2009:15 «Skjult informasjon – åpen kontroll» den 26. juni 2009. I kapittel 20 ble trafikkdata som metode gjennomgått. Utvalget vurderte at politiets bruk av trafikkdata ikke burde være gjenstand for noen innstramming av hensyn til personvernet, men at utlevering kun skulle finne sted ved beslutning om utleveringspålegg etter straffeprosessloven § 210, dvs. at ordningen med at Post- og teletilsynet opphever taushetsplikten ble avviklet.

Den 21. desember 2009 presenterte Nasjonal sikkerhetsmyndighet «Nasjonal strategi for cybersikkerhet». Strategien trekker opp hovedlinjene for videreutvikling av nødvendig samordnende og sektoroverveiende tiltak for helhetlig beskyttelse av kritiske IKT-systemer mot alvorlige hendelser. Tiltak nr. 17 gjelder datalagring:

«Sikre mulighet til nødvendig lagring av data ved hendelser med tanke på å muliggjøre effektiv etterforskning … Etterforskning av datakriminalitet krever data. Om slike data slettes tidlig vil muligheten for å etterforske effektivt hemmes. Det er dessuten en samfunnsmessig utfordring om cyberspace – som vi alle blir mer og mer avhengig av – blir oppfattet som et lovløst rom. Samfunnet må derfor legge til rette for en effektiv etterforskning».

Strategien var på offentlig høring med høringsfrist den 25. juni 2010. Forsvarsdepartementet og Justisdepartementet arbeider nå videre med å følge opp strategidokumentet.

5.4.3 Nærmere om internasjonale forpliktelser og internasjonalt politi- og påtalesamarbeid

Utenriksdepartementet har i sitt høringsinnspill vist til omfattende internasjonalt samarbeid Norge forholder seg til. De peker på en rekke uttalelser og anbefalinger fra internasjonale organer, og internasjonale avtaler som Norge har undertegnet. I det følgende vises det til enkelte av disse anbefalingene og konvensjonene. Disse pålegger ikke medlemslandene noen generell plikt til å lagre data, men har opplysningsverdi i et videre perspektiv hva gjelder behov for data.

I FN-resolusjon 55/63 av 22. januar 2001 uttrykte generalforsamlingen bekymring for at teknologiutviklingen har skapt nye muligheter for kriminell atferd, særlig kriminell utnyttelse av informasjonsteknologi. Generalforsamlingen har gitt denne anbefalingen (pkt. 1 f):

«Legal systems should permit the preservation of and quick access to electronic data pertaining to particular criminal investigations».

Som ledd i bekjempelsen av datakriminalitet (cybercrime) pålegger Europarådets konvensjon om datakriminalitet av 23. november 2001 medlemsstatene å gjennomføre flere tiltak for å sikre elektroniske data. De relevante bestemmelser er art. 16 (hurtig sikring av lagrede, elektroniske data), art. 17 (hurtig sikring og delvis utlevering av trafikkdata), art. 18 (pålegg om utlevering av data), art. 19 (ransaking og beslag av lagrede, elektroniske data) og art. 20 (innhenting av trafikkdata i sanntid). Datakrimutvalget utredet forpliktelsene etter konvensjonen i to delutredninger (NOU 2003:27 og NOU 2007:2), og Norges forpliktelser etter konvensjonen anses oppfylt (jf. kap. 5.4.2).

Hva gjelder beskyttelsen av barn, pålegger FNs konvensjon om barnets rettigheter av 20. november 1989 partene «å beskytte barnet mot alle former for seksuell utnytting og seksuelt misbruk. For dette formål skal partene treffe alle egnede nasjonale, bilaterale og multilaterale tiltak for å hindre» at barn utsettes for seksuelle krenkelser som nevnt (artikkel 34 bokstav a til c). Av Europarådets konvensjon om beskyttelse av barn mot seksuell utnytting og seksuelt mis-

bruk av 12. juli 2007 fremgår i art. 10 nr. 2 bokstav b):

> «Each Party shall take the necessary legislative or other measures to set up or designate … mechanisms for data collection or focal points, at the national or local levels and in collaboration with civil society, for the purpose of observing and evaluating the phenomenon of sexual exploitation and sexual abuse of children, with due respect of the requirements of personal data protection».

Det internasjonale politi- og påtalesamarbeidet har de senere år fått stadig større betydning, især hva gjelder bekjempelsen av kriminalitet som begås ved hjelp av elektronisk kommunikasjon eller som begås på Internett.

Utenriksdepartementets betraktning er at datalagringsdirektivet «bygger på en felles europeisk trusselvurdering, hvor oppfatning av nødvendighet og proporsjonalitet ikke kan ses som et rent nasjonalt anliggende, løsrevet fra en felles erfaringsbakgrunn». De høringsinstanser som har uttalt seg om det europeiske og internasjonale politi- og påtalesamarbeidet har samstemmig gitt uttrykk for at dette samarbeidet er viktig, og i noen sammenhenger, avgjørende.

Utenriksdepartementet uttaler videre at tilgang til elektroniske data utgjør

> «et element i det felles europeiske politi- og strafferettslige samarbeidet, hvor forutsetningen er at rettshåndhevende myndigheter i et land skal ha mulighet til å innhente relevant etterforskningsmateriale fra samarbeidende land, særlig for å kunne bekjempe terrorisme og alvorlig grenseoverskridende kriminalitet. Dersom Norge avskjærer muligheten for å benytte spor fra elektronisk kommunikasjon i etterforskningen av alvorlig kriminalitet, vil det derfor kunne ha betydning for mulighetene til etterforskning også for rettshåndhevende myndigheter i samarbeidende land, i den grad det viser seg å være behov for å søke elektroniske spor hos en tjenestetilbyder i Norge».

Høringsinstanser fra politi og påtalemyndighet uttaler at manglende tilgang til elektroniske data skaper vanskeligheter for norske politimyndigheter i det internasjonale politisamarbeidet, og at konsekvensene kan bli at Norge blir mindre attraktive å samarbeide med i slike saker. Særlig uttalt er manglende lagring av abonnementsopplysninger om IP-adresser som er eldre enn tre uker.

Pågripelsen av hovedmannen i den til nå største kriminalsak i Norge – Nokas-ranet – var et direkte resultat av et vellykket samarbeid med spanske politimyndigheter. Pågripelsen fant sted den 5. april 2005, nøyaktig ett år etter ranet. Hovedmannen ble lokalisert gjennom utveksling og identifikasjon med spansk politi av IP-adressen mannen brukte da han sendte e-post til sine kontakter i Norge fra tilfluktsstedet i Malaga. Det vises også til norgeshistoriens største narkotikasak «Operasjon Broken Lorry», hvor norsk politi avdekket et narkotikanettverk som opererte i hele Europa. Etterforskerne hadde et omfattende samarbeid med nederlandsk politi, som bl.a. utleverte trafikkdata for flere av de mistenkte (omtalt i kapittel 5.4.7.2).

5.4.4 Nærmere om alternativer til bruk av historiske data

5.4.4.1 Beslag

Ting som antas å ha betydning som bevis i saken, kan beslaglegges, jf. straffeprosessloven § 203. Særlig for mobiltelefoner og datamaskiner er dette aktuelt samtidig som politiet setter i verk beslutning om ransaking eller pågripelse, jf. straffeprosessloven § 206 første ledd. Siktede kan kreve spørsmålet om opprettholdelse av beslaget inn for retten, som avgjør dette ved kjennelse, jf. straffeprosessloven § 208.

I mange saker har slike beslag i følge politiet avslørt et langt større sakskompleks og et omfattende nettverk eller organisasjon. Eksempler på dette er beslaget av datamaskinen til siktede i sedelighetssaken «Operasjon Buddy» (kapittel 5.4.7.3) og beslaget av mobiltelefonen i narkotikasaken «Operasjon Broken Lorry» (kapittel 5.4.7.2). I saker av mindre omgang kan denne typen beslag være tilstrekkelig for å få saken nødvendig belyst for videre behandling, uten at det er nødvendig med ytterligere innhenting av lagrede data.

Tilfanget av data fra slike beslag kan etter det politiet opplyser være tilfeldig og begrenset. For det første kan siktede kvitte seg med mobiltelefonen eller datamaskinen sin, eller han sørger for å slette inkriminerende data. For det annet kan loggføringen av trafikken av meldinger og samtaler på apparatet være begrenset, slik at etterforskerne ikke får tilgang til relevante trafikkdata noe lengre tilbake i tid. For det tredje er data om lokalisering normalt ikke tilgjengelig på mobiltelefonen. For det fjerde kan siktede ha etablert ruti-

ner for bruken av mobiltelefonen eller datamaskinen slik at det ikke er relevante data å hente (jf. kapittel 5.4.5).

5.4.4.2 Sikringspålegg

Påtalemyndigheten kan som ledd i etterforskning gi pålegg om sikring av elektronisk lagrede data som antas å ha betydning som bevis, jf. straffeprosessloven § 215 a første ledd. Sikringspålegget gjelder for et bestemt tidsrom, høyst 90 dager, og kun for data som allerede er lagret. Sikringspålegg er omtalt i kapittel 12.1 og i høringsnotatet kapittel 2.4.1.

Sikringspålegg er en målrettet etterforskningsmetode, og forutsetter at etterforskerne kan utpeke de personer og de data som skal sikres. *Kripos* uttaler at Telenor og NetCom mottar ca. 10-20 anmodninger om sikringspålegg årlig, og at metoden hovedsakelig er aktuell overfor tilbydere som sletter før utløpet av fristen de har tillatelse til å lagre data, og ved tidkrevende anmodninger om utlevering av data til utenlandske politimyndigheter. For øvrig er metoden i følge Kripos sjelden aktuell i dag, siden behandlingstiden hos Post- og teletilsynet og hos tilbyderne er ganske kort. Data slettes i liten grad mens uthentingsprosessen foregår.

I en etterforskning som tar tid kan det i følge politiet være vanskelig å vite i starten hvilke data som må sikres. Når etterforskerne vet dette, kan data ha blitt slettet med dagens lagringspraksis. For det annet er sikringspålegg som metode svært sårbar overfor kriminelles mottiltak mot datalagring, jf. kapittel 5.4.5. Et tredje forhold er at også innholdsdata kan sikres, noe som gjør tiltaket betydelig mer personverninngripende.

5.4.4.3 Kommunikasjonskontroll

Bestemmelsene om kommunikasjonskontroll i straffeprosessloven omfatter både kontroll av innholdet i kommunikasjonen (kommunikasjonsavlytting jf. straffeprosessloven § 216 a) og tilgang til trafikkdata (straffeprosessloven § 216 b). Kommunikasjonskontroll etter § 216 b annet ledd, bokstav d gir tilgang til historiske, samtidige og fremtidige trafikkdata, herunder lokaliseringsdata (innholdsdata er ikke omfattet, se kapittel 12.1). Metoden er målrettet, siden det må foreligge skjellig grunn til mistanke mot «noen», og vilkårene er ellers strenge (jf. første ledd bokstav a og b). Normalt vil bestemmelsen anvendes i saker hvor etterforskningen er fremadrettet («proaktiv» etterforskning). Siden politiet på forhånd må vite hvem de skal ha utlevert historiske, samtidige eller fremtidige data på, er metoden sårbar for kriminelles mottiltak (se kapittel 5.4.5). Operasjon Andromeda er et eksempel på en sak hvor etterforskerne unnlot å benytte kommunikasjonskontroll pga. de mistenktes stadige bytte av telefonabonnement m.v. (omtalt i kapittel 5.4.7.2).

5.4.5 Nærmere om omgåelse av datalagringsdirektivet

Etterforskere opplever at en del kriminelle benytter metoder for å unngå å bli sporet når de benytter elektronisk kommunikasjon. Enten ved å benytte elektronisk kommunikasjon som ikke lagres (for eksempel internettbaserte sosiale medier) eller ved å benytte sporbart kommunikasjonsutstyr som ikke er registrert på den kriminelles identitet (for eksempel uregistrerte kontantkort og internettkaféer). Særlig i narkotikasaker og generelt i saker med kriminelle nettverk opptrer omgåelsesmetoder, eksempler på dette er «Operasjon Broken Lorry», «Operasjon Andromeda» (kapittel 5.4.7.2) og Nokas-saken (kapittel 5.4.7.8). Kriminelle nettverk vil normalt være avhengige av å kommunisere elektronisk. Kommunikasjonen er en risiko siden den i seg selv kan lede til avsløring, derfor vil enkelte bruke kommunikasjonskanaler som er beskyttet mot avsløring. *Willassen* uttaler (s. 40-41):

> «Det kriminelle miljøet er i stor grad kjent med at det foretas kommunikasjonskontroll og uthenting av kommunikasjonsdata i forbindelse med politiets etterforskning. Dette har resultert i mottiltak mot slik bevisuthenting fra de kriminelles side. Slike mottiltak kan involvere bruk av kontantkort som er registrert på falske navn, jevnlig bytte av kontantkort og telefoner, samt at man jevnlig kvitter seg med telefoner og kontantkort for å forhindre at disse blir avdekket ved beslag.»

Omfanget av kriminalitet som forblir uoppdaget som direkte følge av at det benyttes ikke sporbare kommunikasjonskanaler, er ukjent, men det må kunne legges til grunn at omfanget ikke er ubetydelig. Når hensikten med datalagringen er å sikre spor med tanke på kriminalitetsbekjempelse, er en situasjon hvor kriminelle unngår sporbar elektronisk kommunikasjon noe man må være oppmerksom på med tanke på direktivets effektivitet.

Ifølge *Riksadvokaten* viser erfaringen at en rekke personer som begår alvorlig kriminalitet, benytter kommunikasjon som fanges opp. Dessu-

ten begås en del kriminalitet i affekt, uten noen planlegging på forhånd. *Kripos* viser til at det ble hevdet kriminelle ville bruke hansker da fingeravtrykksundersøkelser ble innført på begynnelsen av 1900-tallet, men at slike undersøkelser stadig oppklarer et betydelig antall saker. Om «mottiltak» i form av hyppig bytte av telefonnummer uttaler *Willassen* (s. 41):

> «Disse mottiltakene er imidlertid ressurskrevende å gjennomføre, og lider av den svakhet at det nye nummeret må kommuniseres til alle kommunikasjonspartene hver gang man bytter nummer. Erfaring viser at det ofte er mulig å benytte kommunikasjonsdata som bevis på aktivitet i kriminelle nettverk selv om brukerne har foretatt nevnte mottiltak.»

Kripos viser til at man ikke kjenner noen straffesak hvor de involverte var mer bevisst på ikke å etterlate seg elektroniske spor, enn i Nokas-saken. Til tingretten forklarte de domfelte at de stadig ble instruert om ikke å bringe med egen mobiltelefon til ransområdet under planleggingen av ranet. Under ranet ble det brukt egne «ranstelefoner» som de domfelte kvittet seg med etterpå. Enkelte av de involverte hadde stor teknisk kunnskap om politiets metoder, herunder forholdet til basestasjoner og basestasjonssøk, og det ble også beslaglagt avansert teknisk utstyr for å blokkere kommunikasjon («jammer»). Likevel ble gjerningspersonene innhentet av politiets systematiske metoder. Under en bag i en bil som de senere domfelte hadde senket i Drammensfjorden, fant politiet et SIM-kort som kunne knyttes til én av gjerningspersonene. Hovedmannen ble pågrepet som følge av at etterforskerne i samarbeid med spansk politi kunne identifisere IP-adresse fra e-poster han hadde sendt fra Spania. I tingrettens dom avslørte retten stadig motstrid i de siktedes forklaringer om hvor de hadde oppholdt seg, på grunn av lokaliseringsdata som indikerte at de hadde vært i nærheten av lovbruddet. I dommen beskrives kontaktmønsteret mellom de siktede ut fra trafikkdata som etterforskerne fikk innhentet. Tingretten merket seg også at en av ranernes «omgåelsesmetoder» også ble en iøynefallende fellesnevner for de involverte: Alle deres personlige mobiltelefoner hadde ingen inn- eller utgående telefontrafikk den aktuelle helgen, sammenlignet med dagene like før og etterpå.

Et enkelt «feiltrinn» kan være nok til å avsløre et kriminelt nettverk, eksempelvis ved at én av deltakerne i et ubetenksomt øyeblikk plasserer SIM-kortet i sin identifiserbare mobiltelefon. Bruk av data er ett av flere verktøy etterforskerne har tilgjengelig. Det vil være saker som ikke kan avsløres ved bruk av data, men hvor de kriminelle etterlater seg spor som avsløres av andre etterforskningsmetoder, for eksempel DNA- og fingeravtrykksspor.

5.4.6 Nærmere om behovet for data og ulike typer datas betydning

5.4.6.1 Om Post- og teletilsynets praksis for fritak fra taushetsplikt

Post- og teletilsynet har hittil med hjemmel i straffeprosessloven behandlet anmodninger om fritak fra taushetsplikten etter ekomloven § 2-9 med henblikk på utlevering.

I høringsnotatet omtalte departementene Post- og teletilsynets praksis knyttet til behandling av anmodninger om opphevelse av taushetsplikten, og redegjorde for tilsynets erfaringer. I kapittel 2.5 i høringsnotatet viste departementene til tall på politiets begjæringer til Post- og teletilsynet om opphevelse av taushetsplikten. Opplysningene fremgikk for perioden 2001 til 2008, og det fremgikk at antallet hadde ligget stabilt på omtrent 1.900 begjæringer årlig siden fra 2004 til 2008. Hver enkelt begjæring kan gjelde flere identiteter/brukere.

Departementet har i forbindelse med vurderingen av høringsinnspillene innhentet ny og oppdatert informasjon fra Post- og teletilsynet. For året 2009 har Post- og teletilsynet behandlet totalt 2015 anmodninger fra politiet. Post- og teletilsynet har gitt fritak i 1796 av disse sakene og avslag i 219 av sakene.

Tilsynet har siden 1. januar 2010 ført en mer detaljert statistikk enn tidligere vedrørende tilsynets behandling av saker om fritak fra taushetsplikten. Tilsynet har oversendt sin rapport til Samferdselsdepartementet som viser statistikk som gjelder for perioden 1.1.2010 til 17.09.2010. Det fremgår av rapporten at Post- og teletilsynet i denne perioden har behandlet 1418 anmodninger om fritak fra tilbydernes taushetsplikt etter ekomloven § 2-9. Tilsynet har i 178 av disse tilfellene innhentet ytterligere skriftlig informasjon for å kunne vurdere anmodningene, og i tillegg har det blitt innhentet ytterligere informasjon per telefon for 337 anmodninger. Reelt antall anmodninger som Post- og teletilsynet har mottatt anslås å være 1240. Dette korrigerte tallet er funnet ved å trekke fra antall tilfeller hvor tilsynet har innhentet ytterligere informasjon skriftlig fra det totale antall anmodninger som er registrert. Årsaken til at det totale antallet anmodninger må korrigeres,

er at tilsynets statistikkverktøy er utarbeidet for å vise den totale arbeidsmengden som anmodningene om fritak fra taushetsplikten utgjør. Når tilsynet har mottatt svar etter en skriftlig innhenting av ytterligere informasjon, vil det vises som en ny anmodning i tilsynets statistikk.

Videre viser statistikken at av de innkomne anmodningene har Post- og teletilsynet gitt fritak fra tilbydernes taushetsplikt i 1129 tilfeller. 66 anmodninger har resultert i avslag. I 45 tilfeller ble anmodningen avskrevet før realitetsavgjørelse etter tilbakemelding fra den eller de som anmodet om fritak fra tilbydernes taushetsplikt. Det opplyses at en anmodning om fritak tilbyders taushetsplikt om trafikkdata normalt omfatter flere enn ett telefonnummer.

Det er anmodet om fritak fra tilbydernes taushetsplikt for å få tilgang til trafikkdata i 1037 tilfeller. Tilsynet har gitt fritak fra tilbyders taushetsplikt for utlevering av trafikkdata for 2125 telefonnumre. Av disse har det blitt gitt fritak for hele lagringsperioden i 67 % av tilfellene. Lagringsperioden har i henhold til konsesjoner gitt av Datatilsynet vært avgrenset til tre og fem måneder avhengig av hvorvidt det er månedsvis eller kvartalsvis fakturering.

Det er anmodet om fritak fra tilbydernes taushetsplikt for å få tilgang til informasjon fra basestasjonssøk i 215 tilfeller. Tilsynet har i den angitte perioden ovenfor gitt fritak fra tilbydernes taushetsplikt for å utgi resultat fra basestasjonssøk på 260 lokasjoner. Gjennomsnittlig tid for disse basestasjonssøkene er på 4,3 timer per lokasjon, totalt 1110 timer.

Det er anmodet om fritak fra tilbydernes taushetsplikt for å få utlevert PUK-kode i 179 tilfeller. Post- og teletilsynet har gitt fritak fra tilbydernes taushetsplikt for utlevering PUK-kode til 301 telefonnumre. Normalt omfatter anmodninger om fritak fra tilbyders taushetsplikt om PUK-kode flere enn ett telefonnummer.

I perioden fra 1. april til 17. september 2010 har Post- og teletilsynet i tillegg registrert hvilken strafferamme de angjeldende anmodninger er knyttet til. I denne perioden har tilsynet registrert seks anmodninger hvor strafferammen for det angitte straffbare forholdet er under 3 år, eller det straffbare forhold ikke omfattes av opplistingen av lovbrudd som er foreslått som alternativer til det generelle kravet om at handlingen skal kunne medføre fengsel i 3 år eller mer i departementenes høringsnotat om datalagring datert 8.1.2010.

Post- og teletilsynet har mottatt bare to anmodninger hvor begrunnelsen er behov for tilgang til trafikkdata fra IP-adresser.

Tilsynet har gitt fritak fra tilbydernes taushetsplikt i 54 tilfeller der den taushetsbelagte informasjonen gjelder den fornærmede i et straffbart forhold. Slike fritak gis i henhold til tilsynets praksis nesten utelukkende når den fornærmede ikke selv er i stand til å samtykke til utlevering av den taushetsbelagte informasjonen.

Post- og teletilsynet har ikke registrert anmodninger fra andre enn politiet i ovenfor angitte periode.

Videre har departementet mottatt utdypende informasjon fra Post- og teletilsynet som belyser statistikken gjengitt ovenfor. Tilsynet opplyser at statistikken viser utfallet etter tilsynets realitetsbehandling. Det kan derfor ikke utledes at politiet har avgrenset tidsperioden i 33 prosent av anmodningene vedrørende trafikkdata. I mange av sakene som registreres med innvilgelse for en avgrenset periode har det innledningsvis blitt bedt om all lagret trafikkdata, men etter innhenting av opplysninger, har anmodningen blitt endret til en periode avgrenset i tid eller at tilsynet kun har gitt samtykke for en avgrenset periode. Det opplyses også at tilsynet det siste året har skjerpet inn praksisen rundt kravet til begrunnelse for den periode det anmodes om fritak for. Tilsynet har opplevd at politiet gradvis i større grad har bedt om trafikkdata fra mer avgrensede perioder og mener at tilsynets skjerpede praksis som beskrevet, kan ha vært årsak til dette.

I følge tilsynets opplysninger har det ikke har vært ført statistikk for andre detaljer vedrørende fritak fra taushetsplikten enn det som er belyst ovenfor.

5.4.6.2 Kategorier av elektroniske data

I datalagringsdirektivet art. 5 er data som etter art. 3 skal lagres, inndelt i ulike kategorier. *Kripos* deler data inn i *personspesifikke* og *stedsspesifikke* spor. De personspesifikke sporene er utskrifter som knyttes til en bestemt person eller et bestemt telefonnummer eller dataanlegg, mens de stedsspesifikke sporene er spor som knytter seg til et bestemt geografisk område (for eksempel en oversikt over all telefontrafikk i nærheten av et drapsåsted). Begge sportypene har stor betydning for etterforskningen. Kripos skriver om personspesifikke og stedsspesifikke spor:

> «De personspesifikke sporene er i hovedsak utskrifter som viser historisk trafikk for et bestemt telefonnummer eller hvem som har benyttet et bestemt dataanlegg (IP-adresse – abonnementsdata). Telefonutskriftene gir i

hovedsak to typer opplysninger; hvem mistenktes/fornærmedes/vitnets telefon har vært i kontakt med og hvor telefonen har befunnet seg når samtaler er foretatt (basestasjon). Denne typen opplysninger er av stor betydning blant annet for å kontrollere forklaringer og for å avdekke ytterligere impliserte i saken. Utfordringen med personspesifikke spor er å avdekke hvilke telefonnummer / IP-adresser som er relevante før dataene går tapt. De mistenkte er klar over at politiet bruker denne typen spor, og forsøker å vanskeliggjøre politiets etterforskning ved hyppig bytte av telefonnummer, benytte telefonnummer registrert på andre personer (ofte fiktive personer) og ved at det brukes bestemte nummer kun for én straffbar handling. Andre personspesifikke spor som brukes i etterforskning (som ikke er trafikkdata) er eksempelvis utskrift av mistenktes bankkonto, utskrift av bompengepasseringer fra mistenktes bil, bruk av betalingskort/nøkkelkort osv […].

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

Willassen skiller mellom «sporing» og «annen bevisuthenting» (s. 6-7). Ved sporing forsøker politiet å finne ut hvem som har vært motparten i en kommunikasjon, for eksempel å finne identiteten til avsender av en e-post med barnepornografi. I slike tilfeller kan informasjonen som utleveres fra ekomtilbyderen være avgjørende for at politiet kommer videre, for hvis man ikke kan identifiseres noen gjerningsperson kan det være vanskelig å vite hvordan man kan gå frem for å samle inn ytterligere bevis. Ved annen bevisuthenting har politiet et kjent informasjonselement, for eksempel et telefonnummer, og ber så om utlevering av alle oppringninger til og fra dette elementet. Deretter kan politiet gå gjennom dataene og lete etter elementer som kan ha betydning i saken, for eksempel inngående eller utgående samtaler. I slike situasjoner er som regel minst én gjerningsperson kjent, og bevisene som hentes ut skal tjene som dokumentasjon på tilknytningen mellom flere involverte. Willassen vurderer at det ved sporing vil være tilstrekkelig å få tilgang til koblingen mellom kommunikasjonsadressen – for eksempel telefonnummeret eller IP-adressen – og abonnementet, for å identifisere kommunikasjonsmotparten. M.a.o. er tilgang til abonnementsdata tilstrekkelig i disse tilfellene.

5.4.6.3 Kripos' undersøkelse om politiets bruk av historiske trafikkdata

I mars 2010 gjennomførte Kripos en spørreundersøkelse om bruk av historiske trafikkdata i etterforskning. Grunnlagsmaterialet var 1.450 saker fra 2008 med positiv påtaleavgjørelse. En positiv påtaleavgjørelse betyr at det er utferdiget forelegg eller påtaleunnlatelse, eller det er besluttet å bringe saken inn for retten med siktelse eller tiltalebeslutning. Dette betyr samtidig at det er avgrenset mot saker som fortsatt er under etterforskning. Saksutvalget på 1.450 saker omfatter følgende typer overtredelser av straffeloven:

- Grove narkotikasaker (§ 162 annet og tredje ledd),
- seksuelle overgrep (voldtekt, jf. § 192, og seksuelle overgrep mot barn under henholdsvis 10 og 14 år, jf. § 195),
- drap (§ 233, og legemsbeskadigelse med døden til følge, jf. § 229 siste straffealternativ) og
- grove ran (§ 268, jf. § 267).

Straffesaker som har blitt henlagt og hvor det samtidig ble innhentet elektroniske data, er ikke en del av saksutvalget. Undersøkelsen ble gjennomført elektronisk ved at det er sendt ut e-post til hovedetterforsker med henvisning til rolle, saksnummer, registreringsdato og sakskategori, for å forsikre at respondenten innga svar i en konkret sak, slik at det ikke ble inngitt «generelle» svar om nytten av elektroniske data. Dersom det ikke var registrert hovedetterforsker i Strasak (straffesaksregisteret), ble e-posten sendt til påtaleansvarlig i saken. Av grunnlaget på 1.450 saker ble det inngitt svar i 966 av sakene, dvs. en svarprosent på 67 %.

I det følgende refereres det til noen av de funn som ble gjort. For en fyllestgjørende redegjørelse av undersøkelsen og funnene, vises det til høringsuttalelsen fra Kripos, vedlegg 1.

Respondentene ble spurt: «Ble det innhentet historiske trafikkdata i forbindelse med etterforskningen av denne saken»? I 51,9 % av sakene ble dette besvart med «ja» (48,8 % gjaldt trafikkdata fra mobil- og fasttelefoni, 0,3 % gjaldt IP-trafikk, og 2,8 % gjaldt begge deler). I de saker hvor data ikke ble innhentet, ble respondentene spurt: «Hvorfor ble det ikke innhentet trafikkdata i denne saken»? Svarene var som følger:

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

Respondentene ble spurt: «Hvor enig eller uenig er du i at trafikkdata bidro med informasjon av stor betydning for etterforskningen i denne saken?» Svarene for den enkelte sakskategori (drap, narkotika, ran og seksuelle overgrep) er tilgjengelig i undersøkelsen. For alle kategoriene samlet fordelte svarene seg som følger:

Helt enig	litt enig	verken enig eller uenig	litt uenig	helt uenig
60,7 %	21,8 %	5,6 %	3,4 %	8,6 %

Respondentene ble spurt: «Dersom trafikkdata hadde betydning for etterforskningen i denne saken, hvilke opplysninger bidro det med? (flere svar mulig)». Svarene fordelte seg som følger:

- kontroll av mistenktes/siktedes bevegelser (81,8 %)
- kontroll av opplysninger fremkommet i politiavhør eller andre undersøkelser (76,8 %)
- opplysninger om mistenktes/siktedes kontaktmønster (kontaktanalyse) (75,3 %)
- identifisering av gjerningsperson(er) (54,2 %)
- sjekke personer inn/ut av saken (39,5 %)
- kartlegge personer i et bestemt område (basestasjonsutskrifter) (34,6 %)
- trafikkdata var ressursbesparende for saken ved at andre metoder/undersøkelser kunne utelates (25,7 %)
- annet (4,8 %)

Det ble også stilt spørsmål: «Hvor enig eller uenig er du i at det ville vært relevant å innhente historiske trafikkdata lengre tilbake i tid i denne aktuelle saken med hensyn til» 1) trafikkdata fra mobil-/fasttelefoni 2) IP-trafikk. Samtidig ble respondentene informert: «I dag lagres historiske trafikkdata hos teleselskapene i henholdsvis 150 dager hos Netcom og i 90 dager hos Telenor. IP-trafikk kan lagres i 21 dager». Svarene var:

	helt enig	litt enig	verken enig eller uenig	litt uenig	helt uenig
mobil- og fasttelefoni	50,4 %	9,5 %	15,2 %	3,4 %	21,5 %
IP-trafikk	40,8 %	4,0 %	24,3 %	3,5 %	27,5 %

Kripos innhentet statistikk fra Telenor og NetCom. Tallene viser at politiet innhentet ca. 4.600 til 5.000 utskrifter per år fra konkrete telefonnummer i perioden 2007 til 2009. Basestasjonsutskrifter ble innhentet ca. 250 ganger i 2007 og ca. 300 ganger i 2008 og 2009.

5.4.6.4 Ulike typer data med sakseksempler

I det følgende gjennomgås behovet for de ulike kategoriene data som skal lagres i medhold av ekomloven § 2-7a, jf. datalagringsdirektivet art. 5.

Trafikkdata

Trafikkdata fra telefon er personspesifikke spor (jf. kapittel 5.4.6.2), og gir informasjon om kontakt- og kommunikasjonsmønster til den som har brukt telefonen. Trafikkdata er først og fremst interessant i saker hvor det er flere involverte, eksempelvis saker med kriminelle nettverk, som narkotikaomsetning, grove ran, menneskehandel og annen organisert kriminalitet. Dersom etterforskere har mistanke om at en gruppering står bak én eller flere lovbrudd men kun har mistanke mot én eller noen få, kan analyse av trafikkdata belyse kontaktmønsteret og avsløre nye impliserte. Innhenting og analyse av trafikkdata på *nye* mistenkte vil gi et mer fullstendig bilde av hvordan gruppen har organisert seg. I enkelte saker om organisert kriminalitet vil det i praksis være svært vanskelig å rulle opp en kriminell organisasjon uten å bruke trafikkdata.

Trafikkdata kan være helt avgjørende i saker hvor selve kommunikasjonen utgjør lovbruddet, som i saker om innsidehandel og ulovlig prissam-

arbeid. Et eksempel på dette er dom av 11. juli 2007 i sak om innsidehandel fra Oslo tingrett, hvor det fremgår at samtaletidspunktene fra trafikkdataene satte rammen for de straffbare forhold som fremgår av tiltalebeslutningen (saken er omtalt under kapittel 5.4.7.10). En del kriminelle er bevisste i sin bruk av mobiltelefoner, siden det er kjent at etterforskere benytter trafikkdata. Kjente mottiltak er derfor bruk av abonnement registrert på andre personer, jevnlig bytte av abonnement og telefoner, og jevnlig resirkulering av telefoner for å forhindre at innholdet avsløres ved fysisk beslag. Eksempelvis fra Oslo tingretts dom av 20. juni 2007 (Op Broken Lorry, se kapittel 5.4.7.2):

> «Det fremgår for øvrig av et hjelpedokument utarbeidet av politioverbetjent Rune Reitan at B har disponert fem forskjellige mobilnumre i de ca 6 månedene hvor han beviselig var sterkt involvert i virksomheten. Det fremgår av registrerte samtaledata at de aktuelle simkortene endog har vært benyttet om hverandre. Dette gjelder nettopp for samtaler foretatt 21. februar 2006».

Slike mottiltak er imidlertid ressurskrevende for de kriminelle, og tungvint fordi mistenkte må få formidlet nytt nummer hver gang et skifte skjer. Kommunikasjonskontroll og sikringspålegg er etterforskningsmetoder som er sårbare overfor kriminelles bytte av abonnement, siden metodene på forhånd retter seg inn mot bestemte telefonnummer («proaktiv» etterforskning). Også ved bruk av historisk lagrede trafikkdata kan slikt bytte føre til merarbeid under etterforskningen, men her har etterforskerne den store fordelen at de kan gå tilbake i tid. Men det kan ta tid og analysearbeid å finne frem til det «nye» nummeret, og etterforskningen er spesielt sårbar dersom tilbyders lagringstid er for kort.

Willassen uttaler om trafikkdata fra mobiltelefoni (s. 27):

> «Ut fra det som er opplyst er vanskelig å få inntrykk av i hvor stor grad trafikkdata for mobiltelefoni faktisk bidrar til å oppklare saken. Trafikkdata fra mobil som regel en ekstra beviskilde i tillegg til andre beviskilder som er tilgjengelig. Dette er forskjellig fra IP-sporing, hvor sporingen som regel er avgjørende for å finne gjerningspersonen. Bevisene fra trafikkdataene som er hentet ut presenteres i retten sammen med andre bevis som er avdekket gjennom etterforskningen. Ettersom retten som regel fatter en beslutning ut fra et helhetsbilde av alle bevis som er tilgjengelig kan det derfor være vanskelig å avgjøre hvilken betydning trafikkdata fra mobil har hatt for avgjørelsen. For å få nærmere informasjon om dette måtte man eventuelt gå nærmere inn på avgjørelser hvor trafikkdata for mobiltelefoni hevdes å ha hatt sentral betydning. Dette er ikke gjort i forbindelse med den foreliggende utredning».

Vurderingene av trafikkdata fra fasttelefoni (herunder IP-telefoni/bredbåndstelefoni) er i hovedtrekk sammenfallende vurderingene av trafikkdata fra mobiltelefoni (jf. også Willassen s. 31).

Når det gjelder «mislykkede oppringninger», lagrer ikke tilbyderne dette i dag. De lagrer normalt heller ikke tapte anrop. Det vises til kapittel 8.4.3 for mer om dette. Hos den enkelte bruker vil imidlertid telefonen ofte vise logg over tapte anrop. Bruk av data om tapte anrop innhentet fra teleselskapet er omtalt i bl.a. Nokas-saken i Stavanger tingretts dom (jf. kapittel 5.4.7.8) og i en sak om innsidehandel (kapittel 5.4.7.10).

Det britiske EU-formannsskapet viste i sin undersøkelse til en drapssak i Storbritannia hvor mistenkte ble sjekket ut av saken fordi hans påstand om at han ikke kjente til sin kjærestes dødsfall kunne dokumenteres ved hjelp av elektroniske data om tapte anrop. I timene etter drapet hadde han ringt avdøde 27 ganger uten å få svar, men dette fremkom ikke på loggen på telefonen. Imidlertid var det mulig å fremskaffe opplysninger om tapte anrop hos tilbyder, noe som gjorde at etterforskerne sjekket ham ut av drapssaken.

I saker om terrorhandlinger er data om tapte anrop interessante fordi slike digitale signaler utgjør utløsningsmekanismen for mange typer bomber, og data om dette kan gi etterforskere helt nødvendig innledende spor hvor det har blitt begått en terrorhandling.

Internettdata

Etter datalagringsdirektivet art. 5 nr. 1 a) 2) iii) skal tilbyder lagre navn og adresse på den som fikk tildelt en IP-adresse på kommunikasjonstidspunktet (se kapittel 8.5). Stadig mer av kommunikasjonen skjer med Internett som databærer, eksempelvis e-post og nettsamfunn. I følge politiet har dette ført til at etterforskeres behov for å få identifisert IP-adresser har økt de senere år. Både når lovbrudd skjer ved hjelp av Internett («grooming») og når Internett er åstedet for lovbruddet (elektronisk distribusjon av barnepornografi), er etterforskerne helt avhengige av å kunne identifi-

sere avsenderens IP-adresse, siden den som står bak krenkelsen normalt opptrer anonymt (jf. bl.a. kapittel 5.4.7.4 om internettrelaterte seksualforbrytelser).

Etterforskere opplever stadig at gjeldende lagringstid på maksimalt 21 dager for IP-adresser skaper problemer i saker hvor Internett har vært åstedet for, eller brukt ved gjennomføringen av, et lovbrudd. For det første er dette åpenbart i saker hvor politiet først får melding om et lovbrudd etter at 21-dagersfristen har utløpt, slik at det ikke er noen spor å hente hos tilbyder. En del ofre, særlig barn, bruker gjerne noe tid på å bearbeide et overgrep før anmeldelse kan skje, på grunn av overgrepets traumatiserende virkning. Tilsvarende er slettefristen et problem når norsk politi mottar norske IP-adresser som har blitt brukt til kriminelle handlinger fra sine utenlandske politikolleger. I det følgende refereres det til noen eksempler på saker som høringsinstansene har fremhevet.

Politiaksjon i Mellom-Europa (2009)

I forbindelse med en politiaksjon i Mellom-Europa i juni 2009 fikk Kripos oversendt 709 unike, norske IP-adresser som var benyttet til å utveksle overgrepsmateriale (mot barn). Det betyr at mange personer i Norge har mottatt eller sendt filer med overgrepsmateriale på dette nettverket. På grunn av manglende lagring av trafikkdata var det ikke mulig å iverksette etterforskning mot noen mistenkte i Norge.

Brasiliansk sak (2009)

I begynnelsen av oktober 2009 fikk Kripos oversendt tilsvarende IP-adresser fra brasiliansk politi i forbindelse med en aksjon mot et nettverk for distribusjon av overgrepsmateriale der det var blitt utvekslet filmer av overgrep mot barn. Som følge av dette ble blant annet 121 personer arrestert i Spania. På grunn av manglende lagring av trafikkdata var det ikke mulig å iverksette etterforskning mot mistenkte i Norge.

Sak fra Salten politidistrikt (2009)

I en overgrepssak tok etterforskere beslag i en 35-årings PC, hvor det ble funnet flere mindreårige chattekontakter. Politiet henvendte seg til Microsoft, og fikk utlevert alle 46 IP-adresser til identiteter som mannen hadde chattet med. Da politiet kontaktet tilbyderne for å få identifisert IP-adressene, var det bare 20 av IP-adressene som kunne identifiseres, på grunn av 21-dagersfristen. Dermed kunne ikke politiet gå videre med de 26 andre IP-adressene. Politiet vet at mannen lagret de 26 som sine kontakter, men vet ikke hva de har blitt utsatt for og er ikke i stand til å identifisere dem. Imidlertid dokumenterer beslaglagt filmmateriale at mannen begikk overgrep for mer enn ti år siden.

Selv om tilbyderne har tillatelse til å lagre IP-adresser i 21 dager, betyr ikke dette at alle tilbydere benytter seg av dette. Etterforskere i Kripos har mottatt henvendelser på «tips.kripos.no» hvor etterforskningen ikke har kommet videre på grunn av at enkelte tilbydere sletter IP-logger nesten umiddelbart. For det annet må etterforskerne ofte jobbe seg «bakover» for å nøste opp hvilke personer offeret eller overgriperen har vært i kontakt med, og i mellomtiden går IP-logger tapt. For det tredje må etterforskerne samarbeide med utenlandske politimyndigheter i flere saker på grunn av at offer eller overgriper befinner seg i et annet land. Internasjonalt politisamarbeid er tidkrevende, for eksempel når norsk politi anmoder utenlandsk politi om utlevering av data.

Willassen uttaler om sporing av IP-adresser (s. 16-20):

> «I mange saker av denne type [datakriminalitet og seksuelle overgrep], har det straffbare forholdet utelukkende skjedd via Internett. Den eneste måten å finne frem til gjerningspersonen er da å spore vedkommende på internett. Ved bruk av oppkobling med dynamisk ip-adresse kan dette bare gjennomføres dersom det finnes en logg over kobling mellom ip-adresse og abonnent. Når abonnenten først er identifisert, vil politiet kunne utføre ytterligere undersøkelser, for eksempel ved å undersøke datautstyr hos abonnenten. På denne måten vil det kunne avdekkes hvorvidt det var abonnenten selv som hadde utført det straffbare forholdet, noen andre i abonnentens husstand, eller eventuelt andre (for eksempel naboer ved oppkobling til abonnentens trådløse nettverk). Slike undersøkelser fordrer imidlertid at abonnenten kan identifiseres. Dersom dette ikke er tilfelle, vil det som regel ikke finnes noen mulighet til å komme videre i etterforskningen … Etter utreders oppfatning må det vektlegges at disse opplysningene er avgjørende i de sakene det gjelder».

Lokaliseringsdata

Lokaliseringsdata kan brukes som indisiebevis på at brukeren oppholdt seg på et bestemt sted på et

bestemt tidspunkt, når personen mottok eller sendte sms eller telefonsamtale som gikk via basestasjonen.

Willassen uttaler at lokaliseringsdata ikke behøver å ha noe med selve lovbruddet å gjøre. For eksempel kan gjerningspersonen ha mottatt en tilfeldig tekstmelding ved utførelsen av ugjerningen, som knytter ham til åstedet for forbrytelsen. I så tilfelle kan det være helt tilfeldig fordel om data om lokalisering tilflyter etterforskningen, avhengig av om brukeren deltok i en kommunikasjon eller ikke. Willassen uttaler videre:

> «Det synes å være slik at det i noen sakstyper primært er kommunikasjonsdata som er av interesse, mens det i andre saker primært er lokasjonsdata som er av interesse. Lokasjonsdata i forbindelse med elektronisk kommunikasjon kan i forbindelse med straffesaker brukes som bevis på at vedkommende som kommuniserte oppholdt seg på et bestemt sted til et bestemt tidspunkt, uavhengig av hvem vedkommende kommuniserte med og i hvilken form. Brukt på denne måten blir trafikkdata fra kommunikasjonsleverandører et bevis for oppholdssted på lik linje med vitneobservasjoner, bilder fra overvåkningskamera, fingeravtrykk, biologiske spor og andre tekniske bevis. Dette kan ha stor verdi i mange saker der den straffbare handlingen har skjedd på et konkret sted. Det kan imidlertid innvendes at når lokasjonsdata fra elektronisk kommunikasjon brukes på denne måten, så er ikke bruken relatert til selve den elektroniske kommunikasjonen som er foretatt. Den elektroniske kommunikasjonen som er foretatt trenger ikke å ha noe med forholdet som etterforskes å gjøre. Det er utelukkende informasjon om lokasjonen til den som kommuniserte man er ute etter».

Lokaliseringsdata som hentes om en bestemt person, er personspesifikke spor. Lokaliseringsdata har blitt brukt i flere alvorlige straffesaker, i det følgende vises det til tre eksempler. Oslo tingretts dom av 1. desember 2005 gjaldt gruppevoldtekt (se kapittel 5.4.7.3):

> «Retten legger her særlig vekt på at G utpekte ham, at han var venn av den nå etterlyste, at mobiltelefonutskriften viser at han var i Oslo sentrum i den relevante tidsperioden og da hadde kontakt med den nå etterlyste og F samt at han var i –området fra ca kl 1800 (…) Derimot legger retten til vekt på mobiltelefonutskriften der ringemønsteret for dagene rundt overgrepet viser at det er A som har brukt telefonen. Utskriftene viser at han kom til –området ca kl 2148 som er i den perioden da overgrepene fant sted».

Follo tingretts dom av 16. juni 2008 gjaldt ran og grove tyverier fra eldre:

> «Det bemerkes i denne forbindelse at tiltalte ikke har medvirket til å få saken oppklart. Han har fortsatt å benekte at han har oppholdt seg på gjerningsstedene selv etter å ha fått seg forelagt analysen av samtaledata. Han har ikke villet forklare seg hvorfor han har oppholdt seg i området, ei heller har han medvirket til å finne grem til personer som kunne gitt ham alibi».

Nokas-saken i Stavanger tingretts dom av 10. mars 2006 (se også kapittel 5.4.7.8):

> «Under vitneforklaring i retten fremkom det at Bs forklaring på dette punkt ikke kunne medføre riktighet. Kripos-etterforsker Eriksen … har påvist at sim-kortet som B har forklart at han glemte i brystlommen på kjeledressen i garasjen og følgelig mistet den 13.03.2004, faktisk har vært i bruk på basestasjonen Austbø på Hundvåg i Stavanger 25.03.2004 i tiden kl. 12.38 til 12.40. Dette er med andre ord 12 dager senere og stikk i strid med Bs forklaring på dette punkt … Dertil kommer at Es forklaring om at han brakte ranstelefonene til Sandnes 10.03.2004 åpenbart er uriktig, jf. det faktum at ranstelefon nr. 4 lørdag 03.04.2004 kl. 15.50 er aktiv på basestasjon Tagtvedt, kl. 19.47 på basestasjon Hundekleiv, kl. 19.49 på basestasjon Mykland og kl. 20.38 på basestasjon Bjørndalen.»

Basestasjonsutskrifter

Basestasjonsutskrifter er stedsspesifikke spor som gir oversikt over all kommunikasjon innenfor et avgrenset geografisk område, dvs. det område basestasjonen dekker. For å avgrense søket, innhentes data for en begrenset tidsperiode. I henhold til Post- og teletilsynets statistikk for 2010 er det per 17. september anmodet om fritak for å få tilgang til informasjon fra basestasjonssøk i 215 tilfeller. Gjennomsnittlig tid for disse basestasjonssøkene er på 4,3 timer per lokasjon. Basestasjonssøk er i følge politiet nyttig i saker som er knyttet til et bestemt åsted og hvor gjerningspersonen er ukjent.

Denne typen søk er mer personverninngripende enn andre former for uthenting av data,

siden slike søk gir trafikk- og lokaliseringsdata for et på forhånd ukjent antall brukere innenfor angitt tid og sted. Basestasjonssøk er også mer ressurskrevende for etterforskere og tilbyder. Ved basestasjonssøk som omfatter et høyt antall personer, må det foretas en nærmere analyse av datamaterialet. Eksempelvis settes det opp en liste med alibikandidater, som senere kontrolleres mot andre opplysninger for utsjekking.

Basestasjonssøk er i følge politiet i større grad egnet som etterforskningsredskap enn som enkeltstående bevis under hovedforhandling, siden søkene «sveiper» opp et på forhånd ukjent antall personer i området. Registrerte brukere kan senere blir gjenstand for utsjekking. Nokassaken (kapittel 5.4.7.8), Baneheia-saken og Orderud-saken (kapittel 5.4.7.6) er eksempler på alvorlige saker hvor det ble gjennomført basestasjonssøk. Basestasjonssøk kan også være nødvendig i ulykkes- og redningsaksjoner, hvor redningsmannskapene ikke har oversikt over hvor mange som befinner seg i området.

Willassen uttaler om basestasjonssøk:

> «Når det gjelder bruk av lokasjonsdata, så er det opplyst at dette i prinsippet kan være interessant i enhver sak som berører en bestemt lokasjon. Uthenting av lokasjonsdata benyttes imidlertid av ressursmessige og proporsjonalitetsmessige årsaker primært i de mest alvorlige sakene. Således er det saker om grov vold, drap og ran som er de mest aktuelle. I disse sakene blir data om mobiltelefoni hentet ut jevnlig, og tjener da som bevis på lokasjonen vedkommende som benyttet telefonen befant seg på. Slik uthenting kan gjøres på bestemte telefonnummer, for eksempel fordi et bestemt telefonnummer er benyttet av en mistenkt. Det er også mulig å hente ut telefondata som er knyttet til en bestemt lokasjon. For eksempel er det mulig å hente ut en liste over alle samtaler som er knyttet til en bestemt basestasjon. Dette innebærer at politiet får en liste over alle telefoner som utførte eller mottak anrop eller sms via den aktuelle basestasjonen. Dette er en aktuell fremgangsmåte i alvorlige saker med ukjent gjerningsperson, for eksempel drap. Listen over mobiltelefonnummer som fremkommer på denne måten er med å dokumentere hvem som befant seg på lokasjonen på dette tidspunktet og er dermed et mulig utgangspunkt i et søk etter mulige gjerningspersoner. I praksis er det imidlertid så mye arbeid forbundet med en slik fremgangsmåte at den bare brukes i de mest alvorlige sakene».

E-post

Lagring av data om e-post i samsvar med datalagringsdirektivet er personspesifikke spor som forteller om kommunikasjons- og kontaktmønster. Etter direktivet art. 5 skal det både lagres data om hvem som har sendt e-post til hvem og på hvilket tidspunkt, og benyttet IP-adresse samt tidspunkt ved innlogging til e-postkonto.

Høringsinstansene har ikke i særlig grad uttalt seg om praksis ved uthenting og behovet for denne typen data. Det fremgår imidlertid av høringsuttalelsene til politi og påtalemyndighet at etterforskere i flere saker ved henvendelser til selskaper som tilbyr e-postkonto internasjonalt («web-basert mail») har mottatt informasjon om benyttet IP-adresse og tidspunkt for innlogging for i saker hvor etterforskerne vil ha identifisert hvem som står bak en e-postkonto. I det følgende vil det bli vist til utredningen fra *Willassen* (s. 34-36). Willassen uttaler om trafikkdata fra e-post:

> «Når det gjelder logg som viser hvem som har sendt epost til hvem og når, så det opplyst fra politiet at denne type logg ikke etterspørres i særlig grad. Årsaken er primært at det ikke er behov for å hente ut en slik logg i etterforskningssammenheng, fordi den samme informasjonen er tilgjengelig [ved å] gå gjennom epostmeldingens meldingshoder og finne ip-adressen meldingen er sendt fra. Det er ikke nødvendig med noen utlevering av trafikkdata for å gjennomføre dette. Når ip-adressen er funnet, kan opprinnelsen av epostmeldingen spores ved hjelp av ip-sporing, jamfør drøftelsen under punkt 5. Dersom situasjonen er den at man ønsker å kartlegge epostaktiviteten til en mistenkt, vil politiet som regel gå frem på en annen måte enn å hente ut en logg over epostaktiviteten. I slike tilfeller begjærer man heller en ransakingsbeslutning, slik at datamaskinen som er benyttet kan beslaglegges … Den teknologiske utvikling ser ut til å gå i en retning hvor mer og mer data er lagret i nettverket og ikke på brukerens personlige datamaskin. En slik utvikling må nødvendigvis medføre at politiet må beslaglegge epost hos kommunikasjonsleverandøren og ikke på brukerens personlige datamaskin. Det vil imidlertid ikke medføre noe økt behov for pliktig datalagring. Ved sentral lagring må dataene nødvendigvis uansett være lagret på en server et sted, og det er derfor ikke et behov for en plikt til slik lagring».

Willassen uttaler om lagring av data om innlogging til e-postkonto:

> «Når det gjelder logg som viser hvem som har logget seg inn på en epostkonto for å lese epost og fra hvilken epostadresse, så er det opplyst fra politiet at denne typen trafikkdata etterspørres i noen grad. Formålet med å hente inn slike data er som regel å identifisere hvem som benytter den spesifikke epostkontoen. Slik innhenting er derfor spesielt aktuelt i forbindelse med epostleverandører som ikke foretar noen kontroll med identiteten til kunden ved registrering av aktuelle epostkonto, slik at kunden kan skrive inn falske opplysninger om navn og adresse. Dette synes i særlig grad å være tilfelle for eposttjenester som tilbys på Internett uten å ha noen tilknytning til andre abonnement. Det synes i mindre grad å være tilfelle for norske internettleverandører. For disse er navn og adresse til innehaver av epostabonnement som regel kjent, fordi eposttjenesten leveres i tilknytning til et bredbåndsabonnement som leveres til en fast adresse. Således er det opplyst fra politiet at man i særlig grad etterspør slike opplysninger fra utenlandske leverandører … Når disse trafikkdataene utleveres, kan politiet identifisere hvem som bruker den aktuelle epostkontoen ved hjelp av ip-sporing, jamfør drøftelsen under punkt 5. Ifølge det opplyste fra politiet er slik identifisering særlig aktuelt ved etterforskning av seksuelle overgrep og datakriminalitet».

Telenor opplyser til *Willassen* at det kun har vært et fåtall henvendelser fra politiet om utlevering av trafikkdata for e-post siden politisvarsenteret ble opprettet på begynnelsen av 2000-tallet. NetCom og NextGenTel opplyser at de ikke kjenner til at det har vært forespørsler om utlevering av slike data i det hele tatt. Politiet har opplyst at logger som viser innlogging til e-postkonti har blitt etterspurt «i noen grad».

5.4.7 Nærmere om saksområder med konkrete sakseksempler

5.4.7.1 Innledning

Behovet for ulike typer data som skal lagres etter direktivet har ulik betydning for de ulike kategorier av lovbrudd. Ved gjennomgangen av den enkelte kategori lovbrudd nedenfor vil det bli vist til eksempler på konkrete saker. Størsteparten av disse sakene er innspill i høringsrunden fra «brukerne» av elektroniske data, politi og påtalemyndighet.

5.4.7.2 Narkotikasaker

Narkotikalovbrudd er den mest utbredte form for organisert kriminalitet. Normalt ligger det et omfattende nettverk bak de fleste former for ulovlig distribusjon av narkotika. Narkotikakriminaliteten er internasjonal, og det er få vitner til lovbruddene. Det er vanskelig å avsløre narkotikalovbrudd, som følge av at virksomheten er utpreget skjult. Siden enhver befatning er straffbar, vil den som sitter med informasjon normalt være innblandet. Elektronisk kommunikasjon – særlig bruk av mobiltelefon – brukes flittig ved omsetning av narkotika. Politiet har flere metoder som kan brukes når bestemte vilkår er oppfylt, eksempelvis kommunikasjonskontroll, romavlytting, provokasjonslignende tiltak, hemmelig ransaking og beslag eller utleveringspålegg med utsatt underretning til siktede. Men mens de nevnte metodene hovedsakelig brukes ved «proaktiv» etterforskning, avdekkes de fleste narkotikalovbrudd ved reaktiv etterforskning. Narkotikalovbrytere er ofte yrkeskriminelle, og bevisste på politiets metoder. Eksempelvis byttes telefonnummer ofte, og registreres på andre identiteter. Det kan ta lang tid å identifisere hvilke telefonnumre de involverte bruker. Ofte viser det seg at lagringstiden er overskredet når telefonnummeret er identifisert. Politiets fokus har de senere årene flyttet seg enda mer mot bakmennene, for å kunne ramme de som har den største profitten. Bakmennene er som regel ikke i nærheten av narkotikaen, og det viser seg at elektroniske data er helt nødvendige for å avsløre dem. For å ta bakmenn er det også nødvendig å samarbeide med utenlandsk politi, noe som også medfører økt tidsbruk.

Operasjon Broken Lorry (2006)

Kripos avdekket i juni 2006 et marokkansk narkotikanettverk som opererte i hele Europa. I samarbeid med flere politidistrikter og andre lands politimyndigheter ble totalt 35 personer domfelt og det ble idømt i alt 289 års fengsel. Åtte ble pågrepet i utlandet og utlevert til Norge. To av bakmennene ble utlevert fra nederlandsk politi, og idømt 21 års fengsel. Det var første gang lovens maksimumsstraff ble brukt i en narkotikasak. Trafikkdata var helt sentrale bevis mot begge bakmennene. I den samme saken ble en av de norske mottakerne først identifisert 8 måneder etter at saken var rullet opp. Dette medførte at relevante trafikk-

data var slettet. Men politiet mottok data fra nederlandske politimyndigheter, hvor lagringstiden er ett år. Fra Oslo tingretts dom av 20. juni 2008:

> «Det fremgår for øvrig av registrerte telefonsamtaler at B, fra det tidspunkt A og KSB reiste fra Rotterdam til Marokko og under dette oppholdet, har en rekke telefonsamtaler med KSB og SO. KSB forklarte at A brukte hans telefon mens de var i Marokko. Videre fremgår det av samtaledata at B har hatt i alt 98 registrerte oppringninger/samtaler med henholdsvis C og D i tidsrommet fra 9. januar til 4. juni 2006 … Retten bemerker at det er en påfallende stor telefonkontakt mellom B og henholdsvis A og hans to yngre tiltalte brødre på kvelden og på natten forut for dette tidspunktet. I denne perioden har B ringt til A syv ganger, til D fire ganger og til C seks ganger. Riktignok er en av de registrerte forbindelsene med A så kort at det neppe er en reell samtale, og det skal bemerkes at noen av registreringene vedrørende brødrene er så korte at heller ikke det behøver å ha vært reelle samtaler».

Operasjon Green Lamp (2008)

Politiet avdekket ca. 50 ulike cannabisplantasjer i Norge. Ved å innhente trafikkdata fra de mistenktes telefoner kunne en sammenligne dataene og få opplysninger om hvem som organiserte opprettelsen og driften av plantasjene. Øvre Romerike tingretts dom av 13. oktober 2008 illustrerer hvordan retten vurderer elektroniske data i sammenheng med øvrige bevis:

> «Retten finner det hevet over enhver rimelig tvil at E har vært en sentral person i opplegget rundt de to plantasjene. Han har fungert som en tilrettelegger og praktisk organisator. Han har disponert bilen som B eier. Retten peker på at han er den eneste i gruppen som snakker flytende norsk … Han har bistått B med kjøpet av huset i X og leiekontrakten i Horten. Trafikkdata fra den telefonen han ble pågrepet, med viser en omfattende telefonbruk via basestasjon som dekker området der huset i X ligger og likeledes via basestasjoner i Horten. Det er videre registrert trafikkdata på telefonen både til og fra de øvrige impliserte i saken, men mest med D og C. E skal dømmes for grov narkotikaforbrytelse».

Operasjon Andromeda (2009)

Kripos samarbeidet med en rekke europeiske politimyndigheter under avdekkingen av et omfattende albansk narkotikanettverk. De mistenkte var svært bevisste i bruken av elektronisk kommunikasjon, byttet hyppig nummer og brukte MSN og Skype. Logger fra det sistnevnte ble avdekket ved fysisk beslag, men på grunn av 21-dagersfristen kunne ikke IP-adresser herfra spores videre. I Oslo tingretts dom av 25. mars 2010 fremgår det at det måtte innhentes ytterligere trafikkdata fra tilbyderne, men at disse var slettet. Siden deler av virksomheten hadde foregått i Sverige, som har ett års lagringstid, kunne *noe* av materialet innhentes.

5.4.7.3 Seksualforbrytelser

I mange av sakene om seksuelle overgrep kjenner offer og gjerningsperson hverandre. Dersom objektive bevis mangler, kan det avgjørende slaget stå ved om offerets eller gjerningspersonens forklaring blir lagt til grunn av retten. Trafikkdata kan kontrollere de involvertes forklaringer med tanke på kontaktmønster. Lokaliseringsdata opplyser om hvilket kommunikasjonsutstyr som har befunnet seg på et bestemt sted på et bestemt tidspunkt. Er overgriperen ukjent, eksempelvis ved serie- og overfallsvoldtekter, er lokaliseringsdata fra basestasjonssøk ofte avgjørende for å finne frem til riktig gjerningsperson.

Operasjon Buddy (2007)

Etterforskningen startet ved at politiet mottok voldtektsanmeldelse mot en 32-årig mann fra Rogaland. Etter en ransaking fant politiet en stor mengde overgrepsmateriale mot barn på den anmeldte 32-åringens PC, herunder bilder og filmer han selv hadde produsert ved å gjøre opptak av samtaler han hadde hatt med jenter i alderen 9-16 år via MSN Messenger mens webkamera var tilkoblet, og mens han instruerte jentene til å foreta seksuelle handlinger foran kamera. Dommen omfattet internettrelaterte seksuelle overgrep mot 46 jenter, i tillegg til samleie med to av dem. *Kripos* uttaler at sporing av IP-adresser sto sentralt for å få identifisert jentene han hadde forgrepet seg mot, samtidig som dette avslørte en medskyldig. Straffen ble ved Høyesteretts dom av 6. februar 2009 satt til fengsel i 5 år og 6 måneder.

Gruppevoldtekt Oslo (2005)

Fem personer ble dømt for grov gruppevoldtekt av en 16 år gammel jente. Trafikkdata var av betydning for å klarlegge om flere av de tiltalte hadde vært på åstedet, og for å kontrollere troverdigheten av deres forklaringer. Alle fem personene ble domfelt i både Oslo tingrett og Borgarting lagmannsrett. Fra Oslo tingretts bevisvurdering i dommen av 1. desember 2005:

> «Videre legger retten vekt på mobiltelefonutskriften der ringemønsteret for den aktuelle perioden viser at det var han selv som brukte telefonen og at han med basestasjon — ringte en femminutters utgående samtale den 18. desember kl. 0219. Retten har nøye vurdert om A kunne ha vært personen som forlot stedet i grålysningen, men utelukker dette. Hadde det vært A som forlot stedet, tilsier hans aktive mobiltelefonbruk at han ville tatt med seg telefonen og brukt den med annen basestasjon i tidsrommet fra han gikk og frem til kl. 1704 da telefonen igjen er i bruk med basestasjon —».

5.4.7.4 Internettrelaterte seksualforbrytelser

Internett er en ny arena og betyr nye muligheter for seksuelle overgrep. Her kan uvedkommende voksne ta kontakt med barn på sosiale midler med formål om å begå overgrep («grooming» jf. straffeloven 1902 § 201 a), seksuelle handlinger formidles i sanntid (webkamera) og rørlige og urørlige elektroniske bilder av seksuelle overgrep kan spres i et ubegrenset antall eksemplarer. Ved «grooming» brukes Internett som et verktøy ved gjennomføringen av lovbruddet, mens ved krenkelser ved bruk av webkamera og spredning av barnepornografi er Internett selve åstedet for lovbruddet. Gjerningsperson og offer kan da befinne seg hvor som helst i verden.

Norsk politi har deltatt i flere koordinerte internasjonale aksjoner for å straffeforfølge overgripere og identifisere ofre for slike overgrep. Ved denne typen aksjoner kan nye ulovlige nettverk bli avdekket. Dette skjer normalt som følge av beslag i data fra mobiltelefon eller datamaskin hos internettbrukere som har blitt identifisert ved en IP-adresse som norsk politi har mottatt fra utenlandsk politi. Politiets mulighet til å identifisere IP-adresser er ofte avgjørende for å avsløre lovbryterne.

I «Faremo-rapporten» (Forebygging av internettrelaterte overgrep mot barn, 30. januar 2007) uttaler arbeidsgruppen i omtalen av datalagringsdirektivet i kapittel 5.1.7: «Uten bruk av trafikkdata i etterforskningen vil risikoen for at overgripere/gjerningsmenn vil gå fri øke radikalt».

5.4.7.5 Menneskehandel og menneskesmugling

Kjennetegn ved menneskehandel og menneskesmugling er at denne kriminaliteten er organisert og internasjonal. Elektroniske spor kan gi opplysninger om bakmenns rekruttering og kontroll av ofrene, reiserute, annonsering av tjenester på Internett, m.v. Det er betegnende at henholdsvis smugling og handel med mennesker har fått hver sin protokoll under FN-konvensjonen mot grenseoverskridende organisert kriminalitet av 11. desember 2002 (Palermokonvensjonen). Konvensjonen art. 20 nr. 1 pålegger medlemslandene å treffe nødvendige tiltak for bekjempelsen av denne typen kriminalitet, og nevner her særskilt elektroniske etterforskningsteknikker.

Europarådets konvensjon av 16. mai 2005 om tiltak mot menneskehandel art. 13 nr. 1 fastsetter at medlemslandene skal tilby en «refleksjonsperiode» når det er «rimelig grunn» til å tro at personen det gjelder er et offer for menneskehandel. I refleksjonsperioden får personen lov til å oppholde seg i landet, og hensikten er at personen kan områ seg til eventuelt «å treffe en informert beslutning om å samarbeide med kompetent myndighet». Refleksjonsperioden er på seks måneder, jf. utlendingsforskriften § 8-3 første ledd, jf. rundskriv fra UDI nr. 2010-141 pkt. 1.1. I denne typen saker opplever etterforskere ofte at personene først henvender seg mot slutten av refleksjonsperioden. På dette tidspunkt vil de elektroniske spor være slettet.

Grov menneskehandel med mindreårig albansk jente (2009)

Tre personer ble domfelt for grov menneskehandel. En 17-årig albansk jente ble utnyttet til prostitusjon. Hordaland politidistrikt uttaler at trafikkdata sto sentralt for å avdekke tilknytninger mellom de siktede, reiseruter og tilknytning til fornærmede, og antar at ingen av de tiltalte ville blitt dømt uten det bevismateriale som ble avdekket gjennom innhenting av trafikkdata. Fra Gulating lagmannsretts dom av 14. desember 2009:

> «Fra klokken 0638 forsøkte [C] flere ganger å ringe B på mobiltelefonen. Ved femte og sjette forsøk, klokken 0640, tastet han først #31#, som medførte at oppringers telefonnummer ikke ble synlig for mottaker. Lagmannsretten

legger til grunn at C etter hvert forsto at A og B var pågrepet av politiet … Da A og B var borte, var han avhengig av å ha telefonisk kontakt med G [fornærmede] i sitt fravær … Et mobiltelefonabonnement ble her opprettet til G i navnet E, og simkortet satt inn i en mobiltelefon».

5.4.7.6 Drap

Kripos' undersøkelse viser at elektroniske data innhentes i 75 % av alle drapssaker. Er gjerningspersonen ukjent, gir elektroniske data viktig informasjon om hvem avdøde kan ha vært i kontakt med den siste tiden, og hvem som befant seg i nærheten av drapsåstedet på det antatte drapstidspunkt. I saker hvor antatt gjerningsperson er pågrepet på ferske spor, vil elektroniske data gi objektive holdepunkter om hans kommunikasjons- og bevegelsesmønster, og dermed bekrefte eller avsløre motstrid til siktedes forklaring, avdekke ytterligere involverte. I drapssaker generelt er det likevel viktigst at politiet sikres tilgang til stedsspesifikke spor og lokaliseringsdata, som kan gi politiet viktig informasjon om vitner.

Orderud-saken (1999)

Tre personer ble drept på Orderud gård i mai 1999. Fire personer ble pågrepet i juni 1999 og senere domfelt for medvirkning til drap. Trafikkdata var et av flere viktige bevis i saken. Trafikkdata som ble hentet ut etter dagjeldende lagringstid på seks måneder og som belyste våpenoverleveringene, ville vært umulig å hente ut i dag med dagens lagringstid på mellom tre og fem måneder. Fra Nes herredsretts dom av 22. juni 2001:

> «Mellom juleselskapet og 3. april 1999 var det hyppige og korte samtaler mellom As og Ds mobiltelefoner. Etter denne datoen har det ikke vært kontakt mellom disse to telefonene. I følge D dreide mange av samtalene seg om at A maste om å få byttet ut den ene pistolen med en revolver eller iallfall noe med grovere kaliber … D har i sine tidlige politiforklaringer vært usikker på tidsangivelsen for denne overleveringen. Han har etter hvert, og da det forelå utskrifter vedrørende telefondata, landet på at overleveringen skjedde natt til 3. april, dvs. natt til påskelørdag 1999».

Baneheia-saken (2000)

To små jenter ble voldtatt og drept i et friluftsområde i Kristiansand i mai 2000. Gjerningsmennene ble pågrepet i september. Hovedmannen ble ved Agder lagmannsretts dom av 13. februar 2002 dømt til forvaring i 21 år, mens Bs anke over straffen på 19 års fengsel ble forkastet ved Høyesteretts kjennelse av 26. august 2002. Av Kristiansand byretts dom av 1. juni 2001 fremgår det at fire tekstmeldinger på hovedmannens mobiltelefon ble generert gjennom en basestasjon som hadde primærdekningsområde vel 300 meter fra åstedet for ugjerningen. Lokaliseringsdata på tekstmeldingene var blant bevisene som retten måtte ta stilling ved avgjørelsen av skyldspørsmålet. I denne saken var andre bevis, især Bs forklaring, andre vitneforklaringer, DNA-bevis og det forhold at hovedmannen samtidig ble dømt for andre seksualovergrep, utslagsgivende ved rettens bevisvurdering.

5.4.7.7 Vinningsforbrytelser

Et tydelig utviklingstrekk de siste ti år er at omreisende utenlandske kriminelle står bak stadig større deler av de alvorligste vinningsforbrytelsene. Problemet har blitt et satsningsområde for politiet, og det samarbeides mellom politidistriktene. Kjennetegn er at denne typen lovbrytere opptrer som yrkeskriminelle og at de er organiserte. For å føre bevis for at gruppen har hatt som formål å opptre som en organisert kriminell gruppe, jf. straffeloven § 60 a, er trafikkdata blant de få objektive tilgjengelige bevis som viser kontakten mellom gruppens medlemmer. Erfaringsmessig erkjenner ikke de pågrepne flere forhold enn de forhold hvor det foreligger fellende bevis. Bevis i form av lokaliseringsdata kan knytte dem til forretninger og eneboliger som har blitt utsatt for innbrudd og tyverier.

«Skrik»-saken (1994)

Det grove tyveriet av Edvard Munchs maleri «Skrik» i 1994 er den eldste straffesaken som omtales i dette kapittelet. Fra Borgarting lagmannsretts dom av 23. august 1997:

> «C og A sto også senere i svært nær kontakt, også i tiden omkring tyveriet av «Skrik». C var således den første A ringte til etter at maleriet var stjålet, nemlig kl 0729 ifølge samtalespesifikasjonen for As mobiltelefon … Som nevnt fremgår det av en liste over samtaler, som er

ringt av A med mobiltelefon, at han lørdag 12. februar 1994 kl. 0729 hadde en samtale på 22 sekunder med C. A har forklart at han ca kl. 0710 ble oppringt av en journalist som fortalte at «Skrik» var stjålet».

Urmakersakene (2009)

En utenlandsk tyveribande ble pågrepet i Haugesund etter et grovt tyveri fra en urmaker («sjokkbrekk«). Modus var den samme som på flere andre steder i landet. Trafikkdata ble viktig for å knytte gjerningsmennene til andre forhold. Gjerningsmennene ble dømt for tilsvarende forhold både i Kongsberg, Stavanger og Haugesund. Totalt ble det stjålet kostbare klokker for ca 4,6 millioner kroner. Her fra Haugaland tingretts dom av 24. februar 2010, hvor bevisbedømmelsen ble stadfestet ved Gulating lagmannsretts dom av 31. august:

> «En sentral del av denne etterforskningen bestod i undersøkelse av samtaledata for de tiltaltes mobiltelefoner … Videre viser gjennomgangen av samtaledata at tiltalte nr. 1, når tiltalte nr. 2-4 fikk problemer etter innbruddstyveriet hos Lervik Ur den 7. juli, hadde flere SMSer med et polskregistrert telefonnummer i Polen. Dette nummeret har en ikke har klart å komme nærmere eieren av. Dette skjedde kl. 0630 om morgenen. I den situasjonen som da forelå tyder det på en kontakt med bakmenn i tilknytning til tyverihandlingene. Det at det er tiltalte nr. 1 som forestår denne kontakten, og ikke en av tiltalte nr. 2-4, viser hans rolle som leder».

5.4.7.8 Ran

Store ran er som regel utført at godt organiserte og gjerne erfarne kriminelle, og avsløringen av gjerningspersonene tar mye tid og ressurser. Informasjonen kommer frem underveis, og i mellomtiden løper faren for at elektroniske data slettes. Nokas-saken viser at sentral informasjon kan komme etter nærmere ett års tid selv etter at «alle» ressurser tas i bruk. Lokaliseringsdata gir informasjon om mistenkte og vitner som befant seg i nærheten av åstedet, samt mistenktes rekognosering av åstedet i forkant. Trafikkdata som objektive bevis er særdeles viktige å sikre når de siktede velger å forklare seg først under hovedforhandlingen (Nokas-saken). Årsaken er at de siktede har store muligheter for å tilpasse forklaringene til hverandre sammenlignet med forklaringer avgitt til politiet under etterforskningen. Sikres ikke slike objektive spor, blir det en stor utfordring for retten å få saken tilstrekkelig opplyst.

Nokas-saken (2004)

Grovt ran av Norsk Kontantservice i Stavanger sentrum og drap på politimann i april 2004. Ranet var nøye planlagt, men likevel var trafikkdata viktig i etterforskningen. Basestasjonsutskrifter gav opplysninger om både vitner i nærheten av åstedet, samt telefoner som gjerningsmennene hadde benyttet. Gjerningsmennenes telefoner var opprettet kun for å brukes til ranet («ranstelefoner»). Telefonene gav likevel opplysninger om adkomst og fluktrute. Trafikkdata gav også viktig informasjon om forberedelseshandlingene (planleggingsfasen). I tillegg ble trafikkdata brukt for å sjekke ut alibikandidater. I Nokas-saken ble også IP-adresser viktig for å identifisere internettkafeér og andre brukersteder for elektronisk kommunikasjon på Internett. Fra Stavanger tingretts dom av 10. mars 2006 (se også kapittel 5.4.6.4):

> «At det har vært nær kontakt mellom D og A også pr. telefon, fremgår av den fremlagte telefonutskrift som viser at det fra desember 2003 til 25.05.2004 har vært til sammen 53 samtaler dem imellom. Ellers har D utstrakt telefonkontakt med flere av de øvrige tiltalte i saken og han har for eksempel fra desember 2003 til 25.05.2004 totalt hatt 307 kontakter med E, 88 kontakter med G, én kontakt med J og 127 kontakter med K, alt basert på de fremlagte utlistinger».

City-ranet i Lillestrøm (1998)

Flere ranere bevæpnet med skarpladde militærvåpen tok seg inn på handlesenter i Lillestrøm om natten. Senere overfalt de og ranet to vektere fra et vaktselskap som var kommet til stedet for å hente dagens omsetning. Ranet bar preg av planlegging og brutalitet. Innhenting av trafikkdata fra basestasjoner gjorde at politiet kunne knytte flere mellommenn til ranet. Senere etterforskning og innhenting av trafikkdata på disse personene gjorde politiet i stand til å pågripe gjerningsmennene. Hovedpersonene ble dømt til henholdsvis 8 og 9 års fengsel. Uten innhenting av trafikkdata på basestasjonen ville politiets etterforskere ikke hatt muligheter til å avdekke gjerningsmennene. Fra Borgarting lagmannsretts dom av 21. november 2001:

«Et mobiltelefonnummer avmerket på en mobiltelefon funnet i et lokale i –gate 10 i Oslo som B disponerte, ble benyttet kort tid etter ranet med basestasjoner Sørumsand og Askim. Dette samsvarer godt med ranernes sannsynlige fluktrute».

5.4.7.9 Datakriminalitet

Datakriminalitet er lovbrudd som er rettet mot data og datasystemer, og lovbrudd hvor datautstyr benyttes som verktøy for å begå handlingen, jf. NOU 2007:2 «Lovtiltak mot datakriminalitet» s. 42. Ved mange former for datakriminalitet finner lovbruddet sted på det elektroniske mediet selv. Vanlige eksempler er innbrudd i datasystemer, dataskadeverk, nettbankbedragerier, kredittkortbedragerier og trusler og sjikane over Internett. Et felles kjennetegn for slike lovbrudd er at etterforskerne står uten andre potensielle bevis enn de som finnes digitalt, siden Internett som utgangspunkt er uten vitner eller fysiske spor. Sporene vil nesten alltid være knyttet til en IP-adresse som ble benyttet ved lovbruddet, og utfallet av en etterforskning vil ofte avhenge av muligheten til å få identifisert IP-adressen som ble brukt. Et annet kjennetegn ved datakriminalitet er at geografisk avstand mellom gjerningsperson og offer ikke er til hinder for gjennomføringen. De som utøver og profitterer på datakriminalitet vet å dra nytte av avstanden. Politiet erkjenner at etterforskning og bekjempelse av datakriminalitet forutsetter utstrakt internasjonalt politisamarbeid.

Tele2-saken (2007)

En 23-årig mann utviklet et dataprogram for å misbruke en kontrollfunksjon i forbindelse med Tele2s internettbaserte løsning for å bestille mobiltelefonabonnement. Gjennom å kjøre dette programmet lyktes han å liste ut personnummer på tusenvis av nordmenn, med senere potensial for urettmessig bruk. Tiltalte ble dømt for datainnbrudd, jf. straffeloven 1902 § 145 annet ledd. Identifikasjonen av IP-adressen var avgjørende for å få avslørt ham, jf. henvisningen til IP-adressen i tiltalebeslutningen (Asker og Bærum tingretts dom av 22. desember 2009):

«I tidsrommet lørdag 28. juli 2007 til mandag 30. juli 2007 på bopel i Asker, via IP adresse NN.NNN.NN.NN, ved bruk av et script benyttet overfor nettsiden til Tele2 Norge AS, matet han inn forhåndsgenererte norske personnumre, hvoretter han hentet ut fra nettsiden ca. 4.830 norske personnavn, inkludert adresse, personnummer og kredittsjekk, til tross for at han ikke hadde lovlig adgang til dette».

5.4.7.10 Økonomisk kriminalitet

Ved enkelte former for økonomisk kriminalitet kan selve kommunikasjonen være det eneste som skiller en straffbar handling fra en lovlig handel. Eksempler er ulovlig innsidehandel og ulovlig prissamarbeid. Dette er områder som kan bli sårbare dersom de ansvarlige myndigheter ikke gis tilgang til nødvendige data, siden elektroniske data, især trafikkdata og IP-adresser, ofte er det eneste som kan indikere om det har funnet sted en kommunikasjon. For øvrig baseres etterforskning av økonomisk kriminalitet på innhenting av bankkontoutskrifter og regnskapsbilag, ransaking og vitneavhør. De som begår økonomisk kriminalitet har ofte store kunnskaper om hvordan spor skal tildekkes.

Innsidehandel (2005)

Fem personer var tiltalt for brudd på verdipapirhandelloven, og to av disse ble dømt til fengsel i ti måneder hver. To personer i samme sakskompleks ble dømt i Nord-Troms tingrett. Oslo tingretts bevisvurdering i dommen av 11. juli 2007:

«Det ble for retten lagt frem logg over telefonkommunikasjon … Det kan være tale om samtaler, oppringninger som ikke blir besvart, beskjeder til telefonsvar og tekstmeldinger … kjøpsordren ble gitt etter at M hadde ringt opp B fra sin faste meglertelefon … Som nevnt ovenfor skal samtaler mellom kunde og megler tas opp på lydbånd; dette for å kunne dokumentere at det faktisk er gitt en kjøps- eller salgsordre, men også av hensyn til myndighetskontroll med virksomheten. Mobiltelefonsamtaler tas ikke opp på bånd, og innholdet kan følgelig ikke etterprøves. Retten finner det ikke tvilsomt at B i løpet av de to nevnte telefonsamtalene ba M om å foreslå kjøp av Ignisaksjer for å dekke over at det dreiet seg om handel basert på innsideinformasjon».

5.4.7.11 Terrorhandlinger

Bekjempelse av terrorhandlinger er nevnt i datalagringsdirektivets fortale punkt 8 til 10. I punkt 9 vises det til at lagrede data har vist seg å være et effektivt redskap blant annet ved etterforskningen av terrorisme. Punkt 10 vises det til uttalelse fra unionsrådet den 13. juli 2005, om fordømmelse av

terrorangrepene mot London, at det var nødvendig snarest mulig å vedta felles rammeverk om datalagring.

Politiloven § 17 b angir oppgavene til Politiets sikkerhetstjeneste (PST), og avgrensningen faller sammen med straffeloven 1902 § 147 a første ledd a) til c), som angir hva som regnes som terrorhandlinger. I hovedsak er PSTs oppgaver forebygging og etterforskning av sabotasje, politisk motivert vold og tvang samt lovbrudd mot statens sikkerhet og selvstendighet. PSTs rettslige grunnlag for tilgang til elektroniske kommunikasjonsdata er politiloven § 17 d, jf. straffeprosessloven § 210 (jf. kapittel 13). Ingen av de øvrige to etterretnings- og sikkerhetstjenester i Norge, Etterretningstjenesten eller Nasjonal sikkerhetsmyndighet, har tilgang til elektroniske kommunikasjonsdata.

En del av PSTs oppgaver er å forebygge og bekjempe terrorhandlinger som er på et forberedende stadium, herunder motvirke og avsløre rekruttering av personer til terrornettverk. Den nye bestemmelsen i straffeloven 1902 § 147 c setter straff for oppfordring, opplæring og rekruttering til terrorhandlinger. Dannelse av terrornettverk foregår over lang tid med bearbeiding. Terrorhandlinger planlegges og utøves uavhengig av landegrenser og ved bruk av moderne informasjonsteknologi. De best organiserte terrornettverk, som vil være avhengige av å kommunisere elektronisk, er også den største trusselen mot borgernes og rikets sikkerhet. Kartlegging av kontaktnett står derfor sentralt i forebyggingen. Internasjonalt samarbeid mellom politi- og sikkerhetstjenestene er ofte helt avgjørende, hvor de samarbeidende tjenester utveksler informasjon – ikke minst elektroniske data – i stor grad.

PST og *Utenriksdepartementet* har vist til internasjonale forpliktelser i bekjempelsen av terrorisme. *Utenriksdepartementet* uttaler:

> «FNs Sikkerhetsråd har ved flere anledninger uttrykt bekymring for at terrornettverk utnytter ulike media, inkludert Internett, for å spre propaganda og oppfordre til terrorangrep (resolusjon 1617 (2005)), og besluttet at forpliktelsen til å fryse økonomiske midler «apply to financial and economic resources of every kind, including but not limited to those used for the provision of Internet hosting or related services, used for the support of Al-Qaida, Usama bin Laden and the Taliban and other individuals, groups, undertakings, or entities associated with them» (resolusjon 1822 (2008), operativ paragraf 4). Se også beslutning av ministerrådet i OSSE, nr. 7/06, 5. desember 2006 – «Countering the Use of the Internet for Terrorist Purposes» og artikkel 5 i Europarådets konvensjon av 16. mai 2005 om forebygging av terrorisme, som kriminaliserer handling med siktemål «å spre eller på annen måte gjøre tilgjengelig for offentligheten et budskap i den hensikt å tilskynde en terrorhandling» – jf. St.prp. nr. 50 (2008-2009)».

5.4.7.12 Annen etterforskning

Politiet skal beskytte person og yte borgerne hjelp og tjenester i faresituasjoner, jf. politiloven § 2 nr.1 og 4. I redningsaksjoner er politidistriktet lokal redningssentral (LRS) og yter bistand til andre offentlige myndigheter, jf. nr. 6. Blant disse er hovedredningssentralen (HRS). I den innledende fasen besitter politiet vanligvis så lite informasjon at det er et åpent spørsmål om saken vil ende med noen påtaleavgjørelse. Sakene registreres i det sentrale straffesaksregisteret (Strasak).

Ulykkesetterforskning

Politiet etterforsker brann og andre ulykker, selv om det ikke er grunn til mistanke om straffbart forhold, jf. straffeprosessloven § 224 fjerde ledd. Hensynet bak slik etterforskning er at samfunnet har behov for å finne ut av årsaken til ulykken, uavhengig av om noen personer eller virksomheter kan stilles til ansvar sivilrettslig eller strafferettslig. Behovet for en best mulig klargjøring er spesielt viktig i alvorlige ulykker innen luft- og skipsfart. Ved flere slike ulykker vil det oppstå behov for å innhente trafikkdata, blant annet for å fastslå tidspunkter ved et hendelsesforløp og for å kvalitetssikre forklaringer fra øyenvitner.

Savnede personer

Når politiet får inn meldinger om savnede personer, er det vanskelig å gå ut fra om personen har blitt utsatt for et straffbart forhold eller om personen har valgt å forsvinne fra nærmiljøet. Mange slike saker meldes til politiet både timer og dager etter det tidspunkt hvor det ble oppdaget at personen var forsvunnet. Erfaringsmessig endrer noen saker med savnede personer status til drapssaker. Riksadvokaten har derfor i rundskriv til politiet og statsadvokatene presisert at det alltid må has for øyet at forsvinningen kan skyldes en straffbar handling og at relevante spor må sikres, for eksempel banktransaksjoner, bompengebrikke fra motorvogn og elektroniske data som trafikkdata og lokaliseringsdata.

Forsvinnings-/drapssak (2005)

Kvinne fra Lillesand forsvant fra Tananger utenfor Stavanger 3. mars 2005. Hun ble meldt savnet av familien ca. en måned senere. Etterforskningen tydet på at saknede kunne ha foretatt samtaler like før hun ble borte, men trafikkdata var slettet på det tidspunkt da saken endret status (dette var før bestemmelsen i straffeprosessloven § 215 a trådte i kraft). Hennes tidligere samboer ble pågrepet for drapet i 2008. Under hovedforhandlingen i Stavanger tingrett (dom av 15. februar 2010) var de manglende trafikkdata et viktig tema. I denne saken fikk ikke politiet tilgang til trafikkdata, fordi det på innhentingstidspunktet ikke var dokumentert at en straffbar handling hadde funnet sted. Liket er aldri funnet. Straffen ble ved Gulating lagmannsretts dom av 8. oktober 2010 satt til forvaring i 15 år.

5.5 Departementets vurdering

5.5.1 Internasjonale forpliktelser og internasjonalt politi- og påtalesamarbeid

Departementet viser til Utenriksdepartementets uttalelser når det gjelder folkerettslige anbefalinger og forpliktelser. Norske lovregler som sikrer lagring av data har berøringspunkter til de oppgitte anbefalinger og forpliktelser som det er vist til. Departementets forslag til gjennomføring av datalagringsdirektivet vil sikre en bedre harmoni med anbefalingene og forpliktelsene.

Når det gjelder det internasjonale politi- og påtalesamarbeidet, har departementet forståelse for bekymringene fra politi og påtalemyndighet. Det internasjonale samarbeidet er basert på gjensidig bistand. I noen saker mottar norsk politi anmodninger om utlevering av elektroniske data, i andre saker er det vi som etterspør andre lands data. Det er uheldig dersom manglende norsk lagring av elektroniske data danner en oppfatning blant våre samarbeidspartnere om at norske politimyndigheter ikke er i stand til å yte nødvendig hjelp når andre land ber om dette i etterforskningen av sine alvorligste straffesaker og saker om terror. Departementet viser til politiregisterloven § 22, som fastsetter at opplysninger kan utleveres til utenlandske myndigheter til bruk i straffesaker, herunder til etterforskning, saksforberedelse, avgjørelse, gjennomføring av avgjørelsen, oppfølgning og kontroll. Opplysninger kan også utleveres til utenlandsk politi- og etterretningstjeneste for å avverge eller forebygge lovbrudd dersom slik utlevering er nødvendig for å verifisere andre opplysninger. Opplysninger kan for øvrig utleveres til, eller på annen måte gjøres tilgjenglig for utenlandske myndigheter, når dette følger av lov eller konvensjon som er bindende for Norge. Et eksempel på det siste er Rådets rammebeslutning av 18. desember 2006 om forenkling av utvekslingen av opplysninger og etterretninger mellom medlemsstatenes rettshåndhevende myndigheter («Det svenske initiativ», 2006/960/RIA).

5.5.2 Alternativer til bruk av historiske data

Når det gjelder beslag, ser departementet at beslag av mobiltelefoner og datamaskiner er en viktig kilde for tilgangen til elektroniske data i flere saker. Beslag som metode utelukker likevel ikke datalagring. De oppgitte sakseksemplene illustrerer at det er samspillet mellom flere metoder som har gitt de store gevinstene ved de større sakene.

Departementet legger til grunn at antallet årlige sikringspålegg er lavt, men at metoden kan være viktig i de saker det gjelder, hvor det er fare for at data slettes. Sammenlignet med datalagring har sikringspålegg klare svakheter som metode, mest åpenbart er dette i saker med ukjent gjerningsmann og i tidkrevende saker hvor opplysninger om involverte tilflyter etterforskningen etter lengre tid.

Departementet mener at innhenting av data i medhold av § 216 b annet ledd bokstav d) er mest aktuelt i saker av forebyggende og fremadrettet karakter, eksempelvis ved terrorhandlinger og alvorlige narkotikasaker. Kommunikasjonskontroll som nevnt utelukker ikke bruk av lagrede data i samsvar med direktivet, men disse metodene kan i samspill optimalisere kriminalitetsbekjempelsen i den enkelte sak. For eksempel kan en analyse av innhentede historiske data gi grunnlag for at politiet innhenter samtidige og fremtidige data på bestemte personer. Departementet vurderer at de omtalte alternativene ikke i tilstrekkelig grad vil kunne erstatte historiske trafikkdata som verktøy for etterforskning og oppklaring av alvorlig kriminalitet.

5.5.3 Omgåelse av datalagringsdirektivet

Departementet ser at en del kriminelle benytter seg av kommunikasjon som ikke er sporbar. Lagringsreglene tar ikke sikte på en løsning hvor absolutt alle elektroniske kommunikasjonsformer kan spores. Mulighetene til å omgå lagring er

heller ikke noe nytt, samtidig som norsk politis erfaring med bruk av data gjennom mange år har bidratt til oppklaring av mange saker, jf. kapittel 5.4.7. Ved gjennomføring av direktivet vil lagringstiden bli forlenget, noe som gir grunn til å tro at flere saker kan oppklares. Når det gjelder terrorhandlinger, har det i de senere år vært en tendens til at små grupperinger og personer som samarbeider med terrornettverk i utlandet, opptrer mindre «gjennomtenkt» under planleggingen, og er lette å avsløre. Samtidig er det svært viktig at slike terrorhandlinger avsløres, siden handlingene er potensielt svært farlige. Departementet viser også til at datalagring som metode er mindre sårbar for kriminelle omgåelsesmetoder enn sikringspålegg og kommunikasjonskontroll (kapittel 5.4.4.2 og 5.4.4.3).

5.5.4 Behovet for data og ulike typer datas betydning

Departementet viser til inndelingen av type data omtalt i kapittel 5.4.6.2. Departementet vurderer at gjennomgangen er egnet til å lette forståelsen av bruken og nytten av data i kriminalitetsbekjempelse. Såkalte *stedsspesifikke* spor reiser betydelige personvernmessige betenkeligheter, siden de knytter seg til et område hvor kommunikasjon skjer, og ikke til en bestemt person som kommuniserer (jf. kapittel 5.4.6.4). Stedsspesifikke spor i form av basestasjonsutskrifter er følgelig en mindre målrettet metode. Til sammenligning er data som brukes til *sporing* spesielt målrettet, siden resultatet av sporingen avslører hvilken identitet som skjuler seg bak et telefonnummer eller en IP-adresse. Sporingen kan være helt avgjørende i noen typer straffesaker, og reiser mindre personvernmessige betenkeligheter. Kombinasjonen av målrettethet/nytte og personvernmessige hensyn av forskjellige data gir seg samtidig utslag i hvilke lovskranker som fastsettes for forskjellige typer data.

Departementet er enig med *Riksadvokaten* i at tallene fra *Kripos*' undersøkelse (kapittel. 5.4.6.3) dokumenterer behovet for lagring av elektroniske data på en god og overbevisende måte. De fire sakskategoriene som lå til grunn for Kripos' undersøkelse, drap, grov narkotikakriminalitet, grove ran og seksuelle overgrep, er straffesakstyper som etter departementets syn er å anse som alvorlig kriminalitet. I det utvalget av saker som Kripos viser til ble det innhentet data i 52 % av sakene. Dette støtter oppfatningen av at elektroniske data er et viktig verktøy i bekjempelsen av alvorlig kriminalitet. Med tanke på at nytten av data ikke alltid synliggjøres i straffedommen, er det interessant at etterforskerne vurderte data som nyttige i 82,5 % av sakene. Respondentene ga i undersøkelsen uttrykk for at det for den angjeldende sak ville vært aktuelt å innhente elektroniske data lengre tilbake i tid enn det som faktisk ble gjort. Dette viser at etterforskere opplever et behov for lengre lagringstid enn det som følger av dagens lagringspraksis.

Departementet mener det kan være vanskelig å måle konkret nytteverdi av *trafikkdata* sammenlignet med saker hvor IP-adresser identifiseres, siden identifikasjon av IP-adresser kan være et helt avgjørende ledd for å få oppklart lovbrudd som er internettrelaterte. Det er liten tvil om at trafikkdata i enkelte saker har hatt avgjørende bevis- og oppklaringsverdi, særlig i saker om organisert kriminalitet og saker hvor kommunikasjonen utgjør kjernen i lovbruddet. Det vises til gjennomgangen i kapittel 5.4.7, hvor det fremgår av flere straffedommer at trafikkdata har hatt betydning for rettens avgjørelse av skyldspørsmålet. Departementet ser det slik at betydningen av data fra *fasttelefonitrafikk* vil være synkront fallende med nedgangen i bruken av slike tjenester. Det er likevel nødvendig at disse data lagres all den tid markedet tilbyr denne form for kommunikasjon. I tillegg kommer at fysisk beslag av fasttelefonapparatet normalt ikke gir politiet noen data, i motsetning til tilsvarende beslag av mobiltelefoner.

Departementet vurderer at informasjon om *tapte anrop* er nyttige i en etterforskning idet de forteller noe om kommunikasjons- og kontaktmønsteret, selv om det ikke ble oppnådd kontakt. Eksempelvis vil etterforskerne av en drapssak også ha nytte av hvem som *forsøkte* å oppnå telefonkontakt med avdøde i timene før døden inntraff, i tillegg til saker som gjelder terrorhandlinger som omtalt.

Departementet er enig i at identifikasjon av bruker bak en *IP-adresse* er avgjørende i saker hvor det er begått kriminalitet på, eller ved hjelp av, Internett. Departementet deler bekymringene for manglende oppklaring av saker hvor angjeldende IP-adresser er eldre enn 21 dager. 21 dager er for kort, også i saker hvor etterforskningen har hatt en god fremdrift. Behovet for identifikasjon av IP-adresser og en lengre lagringstid av koblingen mellom IP-adressen og kundeidentiteten, er dokumentert.

Departementet vurderer at de tre sakseksemplene (kap. 5.4.6.4) godt illustrerer den betydning *lokaliseringsdata* kan ha under rettens bevisvurdering. I tillegg kommer de saker hvor mistenkte gir

en annen forklaring under etterforskningen når lokaliseringsdata blir presentert for ham, eller når politiet sjekker en alibikandidat ut av saken siden lokaliseringsdata viser at han ikke var i nærheten av åstedet på gjerningstidspunktet. Slike tilfeller er viktige, men synliggjøres i liten grad i en straffedom. Nytten i lokaliseringsdata ligger i at slike data er indisiebevis for at en person har vært på et bestemt sted på angitt tidspunkt.

Departementet vurderer at *basestasjonssøk* bør reserveres for de alvorligste sakene. Søkene kan gi adgang til data om kommunikasjonen til et stort antall mennesker, noe som er problematisk personvernmessig. Søkene er mindre målrettede, siden de tar utgangspunkt i en sentralenhet for kommunikasjonen til et ubegrenset antall personer, nemlig basestasjonen. Likevel må politiet sikres tilgang også til slike data når det gjelder svært alvorlig kriminalitet med ukjent gjerningsperson og ved terrorhandlinger. Etter departementets vurdering balanseres hensynene ved at kravet til strafferamme settes høyere for basestasjonssøk enn for tilgang til øvrige data som skal lagres etter direktivet, jf. forslaget til ny straffeprosesslov § 210 c.

Departementet mener behovet for *trafikkdata om e-post* er noe mindre enn behovet for trafikkdata fra taletelefoni, siden etterforskerne kan identifisere avsenderen av en e-post ved å få identifisert IP-adressen som følger med e-posten. Imidlertid gir ikke denne informasjonen etterforskerne noen systematisk oversikt over trafikken fra en e-postkonto. Særlig i saker hvor politiet etterforsker lovbrudd hvor foretak eller organisasjoner er mistenkt, vil slike systematiske oversikter over trafikk fra e-postkonti ha betydning for sakens opplysning. Systematisk oversikt har dessuten stor betydning i saker som gjelder kartlegging av terrornettverk og personer som søker å komme i kontakt med slike nettverk, og hvor tilnærming og planlegging går over lengre tid. I utredningen vises det til at politiet kan ta fysisk beslag i den enkelte datamaskin og på denne måten få full oversikt over trafikken. Til dette vil departementet for det første bemerke at mistenkte ikke sjelden destruerer eller fjerner lagringsmediet før etterforskerne kan gjøre slikt beslag, i likhet med narkotikakriminelle som bytter ut eller fjerner mobiltelefonen for å unngå det samme. For det annet kan etterforskerne ha behov for å få oversikt over trafikkdata fra e-post før brukeren av e-postkontoen blir kjent med at han er mistenkt. For det tredje er fysisk beslag langt mer personverninngripende enn tilgang som begrenser seg til trafikkdata. Ved beslag vil etterforskerne ha tilgang til innholdsdata og til all øvrig private data som måtte være lagret på datamaskinen. Dette vil måtte innebære betydelige mengder overskuddsinformasjon. For det fjerde må etterforskerne i hvert tilfelle ha tilgang til meldingshodet til en e-post som mistenkte har sendt, for å kunne få identifisert avsender på bakgrunn av IP-adressen. På bakgrunn av dette, vurderer departementet at det er behov for å lagre data om avsender og mottaker av e-post samt tidspunktet for kommunikasjonen.

5.5.5 Saksområder med konkrete sakseksempler

Departementet viser til gjennomgangen av de forskjellige saksområdene med sakseksemplene til hvert område. Omtalen av de forskjellige typer saksområder viser at behovene for ulike typer data som skal lagres varierer mellom områdene. Ofte er det et samspill mellom ulike typer data, men utgangspunktet er at bruk av data er en viktig del av helheten, sammen med de andre metodene politiet bruker i etterforskningen av saker. I de fleste sakseksemplene er det vist til rettens vurdering av bevis under skyldspørsmålet. Sitatene i de aktuelle sakene viser klart at data har hatt betydning i bevisvurderingen. Saksomtalen og eksemplene bidrar til større klarhet og forståelse av hvilken betydning lagrede data har i politiets etterforskning.

Enkelte av sakseksemplene er hentet fra de største kriminalsakene de senere år. Det er vanskelig å vurdere utfallet av sakene gitt at etterforskerne ikke hadde hatt tilgang til lagrede data. Det er likevel ingen tvil om at data bidro til å få saken bedre opplyst, og det er sannsynlig at noen saker og impliserte i enkeltsaker ikke hadde blitt gjenstand for pådømmelse. I et mer helhetlig perspektiv er bruken av data et spørsmål om hvilke metoder politiet skal kunne anvende for å inneha og opprettholde evnen til å bekjempe og oppklare alvorlig kriminalitet og terrorhandlinger.

Når det gjelder terrorhandlinger, viser departementet til OSSEs pakt av 7. desember 2002 for forebygging og bekjempelse av terrorisme, hvor medlemslandene etter tiltak nr. 22 forplikter seg til å treffe nødvendige tiltak for å forhindre misbruk av informasjonsteknologi til terroristiske formål. Terrorhandlingene i New York, London og Madrid viser at én enkelt terrorhandling – ut over de umiddelbare tap av menneskeliv og annen skade – alvorlig kan forstyrre funksjonene og strukturene i samfunnet og skape stor frykt blant sivilbefolkningen. Konsekvensene av manglende

avverging og oppklaring av terrorhandlinger kan være alvorlige. PST uttaler at bruk av data som nevnes i datalagringsdirektivet i dag står sentralt for å løse oppgavene som tilligger deres mandat. Under offentlig nødstilstand som truer nasjonen, kan myndighetene treffe tiltak som fraviker pliktene etter EMK art. 8 i den utstrekning situasjonens krav gjør det strengt nødvendig, jf. EMK art. 15 nr. 1 jf. nr. 2 om fravikelse i krisesituasjoner. En slik offentlig nødstilstand kan være en alvorlig terrorhandling mot Norge eller norske interesser som berettiger adgang til å innføre unntakstilstand. Adgangen til å innføre unntakstilstand i Norge antas å følge av konstitusjonell sedvanerett.

6 Personvern

6.1 Innledning

Innføring av bestemmelser om lagring av data fra elektronisk kommunikasjon reiser viktige spørsmål om borgernes personvern. Kommunikasjonen vår, enten den er elektronisk eller ikke, oppfattes av de fleste som svært privat. Data om kommunikasjonen vår forteller mye om oss og nettverket vårt, også selv om det ikke lagres innholdsdata, dvs. hva som kommuniseres, og er derfor noe de fleste ønsker å verne om. Obligatorisk lagring av trafikkdata vil av mange kunne oppleves som en integritetskrenkelse. Pålegg om lagring av trafikkdata for elektronisk kommunikasjon, må derfor følges av gode regler som ivaretar borgernes behov for integritetsvern.

Lovpålagt lagringsplikt har vært diskutert en rekke ganger, blant annet i forbindelse med vedtagelse av lov om elektronisk kommunikasjon 4. juli 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. En viktig del av begrunnelsen har vært prinsipiell motstand mot massiv lagring av opplysninger om alle borgere som «potensielle kriminelle», og at tilbyderne pålegges å lagre data som de ikke selv har saklig behov for i sin virksomhet. Ekomtilbyderne skal altså ikke bare registrere opplysninger til egne administrative formål, men også for politiets behov. 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, samt en rapport om implementering av datalagringsdirektivet i EU-landene. Disse uttalelsene er å finne på *http://www.regjeringen.no/nb/dep/fad/dok/nouer/2009/nou-2009-1/24.html?id=542291*, og *http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp172_en.pdf*.

6.2 Høringsnotatets redegjørelse

Personvern er en grunnleggende verdi i et demokratisk samfunn, og må sees i sammenheng med viktige rettsstatsverdier som rettssikkerhet og ytringsfrihet. Personvern handler både om beskyttelse av personopplysninger som registreres om borgerne, og om integritetsvern. Lov om behandling av personopplysninger 14. april 2000 nr. 31 implementerer EUs personverndirektiv i norsk rett, og inneholder bestemmelser som skal bidra til at personopplysninger behandles på en måte som ikke krenker personvernet. Andre viktige personvernbestemmelser finnes i spesialregelverk, blant annet i form av taushetspliktsregler og spesialbestemmelser om behandling av personopplysninger innenfor bestemte sektorer.

Personvernhensyn, som alle andre grunnleggende rettigheter, må avveies og finne sitt innhold bl.a. i møte med andre viktige samfunnshensyn, herunder hensynet til kriminalitetsbekjempelse. Det må foretas en grundig vurdering av om en lagringsplikt kan forsvares ut fra det hensyn 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 informasjon om og 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, med tilhørende muligheter for 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 informasjonsbildet, 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 nevnt ovenfor, at samfunnets overvåkings- og kontrollnivå skal være så begrenset som mulig. Behandling av personopplysninger skal være nødvendig for å oppnå et legitimt formål. Med utgangspunkt i dette, er det et grunnleggende spørsmål 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. Samlet finnes 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 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.

6.3 Høringsinstansenes syn

Følgende høringsinstanser har uttalt seg generelt om de personvernulemper datalagring kan medføre for borgerne, og den negative effekten lagringen kan ha for borgernes kommunikasjon: *Datatilsynet, Advokatforeningen, Universitetet i Oslo – Senter for menneskerettigheter, Stopp Datalagringsdirektivet, ICJ-Norge, Det nasjonale statsadvokatembetet, Forbrukerrådet, Oslo statsadvokatembete, Politidirektoratet, stiftelsen Elektronikkbransjen, Samfunnsorganisasjonen Demos, Nardo Nidarvoll Arbeiderlag, Fagforbundet Lillehammer, Forbundet El&It, IKT-Norge, NITO, YS, Partiet Rødt, Nei til EUs lokallag i Østfold, Telemark, Troms, Hordaland, Akershus, Vestfold, Sør-Trøndelag* og *Sogn og Fjordane, Kripos, Tele2, Barneombudet, Norsk presseforbund, NRK, FriBit, NUUG, Norsk Målungdom, Folkets høringsuttalelse, Norges Juristforbund privat, NAV, Post- og teletilsynet, Redd Barna, Ventelo, Universitetet i Bergen, Senterungdommen, Norges politilederlag,* samt *Elektronisk Forpost Norge.* Disse merknadene er ikke knyttet til konkrete bestemmelser i lovforslaget, men til innføring av datalagring som sådan.

Datatilsynet uttaler:

> «Datalagringsdirektivet vil innebære en massiv, statlig innsamling og lagring av opplysninger om hvilke personer som til enhver tid kommuniserer med hverandre ved hjelp av elektroniske hjelpemidler, når denne kommunikasjonen skjer og hvor den enkelte da befinner seg.
>
> Opplysningene skal lagres i minst seks måneder. Datatilsynet mener at dette innebæ-

rer en betydelig trussel mot personvernet, både som en individuell rettighet og som et middel for å bevare den tilliten og maktbalansen mellom den norske stat og dens borgere, som er nødvendig i et demokrati».

Datatilsynet uttaler videre:

«Tilsynet mener at spørsmålet om implementering av datalagringsdirektivet først og fremst er et prinsipielt spørsmål, og at det derfor er av underordnet betydning hvordan direktivet eventuelt implementeres (med tanke på for eksempel lagringstid og -sted)».

ICJ-Norge uttaler:

«Etter gjennomgangen ovenfor, mener ICJ-Norge å ha vist at en gjennomføring av DLD representerer en logikk og et inngrep som vil ha dramatiske – og dels uoverskuelige – konsekvenser for flere av våre grunnleggende, demokratiske friheter og for den liberale rettstat som samfunnsform. Tiltaket vil heller ikke være egnet til å nå de mål det er begrunnet i. Implementeringen vil dessuten etter ICJ-Norges oppfatning krenke den enkelte borgers rettigheter etter EMK på flere punkter».

Advokatforeningen uttaler:

«Datalagringsdirektivet pålegger som kjent statene å lagre alle trafikkdata om telefoni- og internettbruk i det enkelte land (men ikke innholdet i kommunikasjonen). Lagring av data i et slikt enormt omfang som direktivet pålegger, innebærer at myndighetene forestår en systematisk og vedvarende «screening» av hele befolkningens bruk av dagligdagse kommunikasjonsmidler. Som myndighetstiltak for å bekjempe kriminalitet er dette noe prinsipielt nytt. Inngrepet i befolkningens private forhold er meget betydelig og faren for misbruk er stor. I tillegg kommer at reglene gjør inngrep i etablerte rettigheter som for eksempel pressens kildevern, ved at det ikke gjøres unntak for lagring av data fra redaksjonslokaler.

Departementet anser dette som et mindre inngripende tiltak enn de etterforskningsmidler man allerede kjenner. Dette er Advokatforeningen uenig i. På grunn av denne nedtoningen av de nye reglenes egentlige prinsipielle sider godtas lagringen alt for lett som proporsjonal, og det åpnes i tillegg for en meget utstrakt bruk av den innsamlede informasjonen, d.v.s. i alle straffesaker med strafferamme på 3 år eller mer hvor trafikkdataene kan *«antas å ha betydning som bevis»,* jf. strpl § 210. I tillegg er det stor fare for misbruk.

Vi står altså overfor en ny situasjon når det gjelder overvåkning av befolkningen. Forslaget reiser således nye og prinsipielt alvorlige spørsmål om forholdet til grunnleggende menneskerettigheter, særlig retten til privatliv som bl.a. er beskyttet av EMK artikkel 8. Det samme gjelder både myndighetenes lagring og bruk av dataene».

Folkets høringsuttalelse, Advokatforeningen, Stopp DLD, Raudt Sogn og Fjordane, samt lokallagene til *Nei til EU i Telemark* og *Østfold,* mener datalagring innebærer overvåking av alle, og dermed svekker rettssikkerheten. *Foreningen FriBit, YS* og *Elektronisk Forpost Norge* viser også til at lagring av trafikkdata er en del av samfunnets massive lagring av personopplysninger, og at lagringen derfor må vurderes i forhold til det totale informasjonsbildet.

Advokatforeningen uttaler:

«Den omfattende registrering av kommunikasjonsdata som direktivet innebærer, berører de aller fleste mennesker og utgjør en prinsipiell og omfattende utvidelse av myndighetenes overvåking av befolkningen.

Det er en teoretisk diskusjon om man skal kalle direktivets regler overvåking eller ikke. Uansett medfører direktivet at det lagres vesentlig mye mer informasjon om oss enn tidligere og uten at det er mistanke om staffbare forhold som begrunner lagringen».

FriBit uttaler:

«I dagens samfunn blir den tilgjengelige informasjonen om hver enkelt borger stadig større. Vi legger igjen spor overalt, og disse sporene blir oftere og oftere tilgjengelige både for påtalemyndigheter og andre medborgere. For hver utvidelse av den tilgjengelige informasjonen blir det lettere å danne et større bilde om hver enkelt borger.

Av hensyn til hver enkelt persons privatliv og personvernet forøvrig bør vi derfor være særs forsiktige med å innføre nye tiltak som utvider informasjonstilgangen. Privatlivet og et tilstrekkelig vern av personlig integritet er nødvendig for menneskers utvikling, og ikke minst for balansen i samfunnet. Det må være anledning til å foreta seg lovlige handlinger i det

offentlige (og private) rom uten nøye avveining for om handlingen kan bli brukt mot en i fremtiden. Uten denne anledningen vil samfunnets og borgernes utvikling stagnere. Man bør merke seg at lovlige handlinger ikke alltid tåler dagens lys».

Norges Juristforbund privat stiller spørsmål ved hvor grensen går for hvilken registrering, overvåking og kontroll vi er villige til å akseptere for et tryggere samfunn. *Barneombudet* spør hva slags samfunn vi ønsker å overlate til våre barn. Ombudet mener faren for at vi går mot et overvåkingssamfunn må vektlegges i denne saken, og viser blant annet til barns rett til et godt oppvekstmiljø.

Det nasjonale statsadvokatembetet (NAST) mener faren for personvernkrenkelser ved gjennomføring av datalagringsdirektivet er betydelig overdrevet, og viser til at det ikke har vært noen store skandaler knyttet til politiets bruk av trafikkdata i etterforskningssammenheng hittil. *NAST* mener videre at innføring av en lagringsplikt vil sikre nødvendig personvern for ofrene for kriminalitet.

NAST uttaler:

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

Politidirektoratet erkjenner at innføring av datalagringsplikt kan oppleves som en krenkelse av personvernet, og at lagringsplikten utgjør et inngrep i personvernet. Direktoratet mener likevel at inngrepet har begrenset rekkevidde, samtidig som det har stor positiv samfunnsmessig betydning.

Politidirektoratet uttaler:

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

Forbrukerrådet, Norsk presseforbund, NRK, EL&IT, FriBit, NUUG, IKT Norge, Norsk Målungdom, ICJ-Norge, Partiet Rødt, samt lokallagene til *Nei til EU i Telemark, Østfold* og *Troms* mener datalagring vil ha en nedkjølende effekt på borgernes kommunikasjon (chilling effect). Muligheten for omfattende kartlegging av kontaktnettverk kan føre til at borgerne opplever utrygghet med hensyn til hvem de kommuniserer med. *NAST* mener argumentet om nedkjølende effekt mangler empirisk grunnlag, og heller ikke er særlig sannsynlig siden det ikke skal lagres data om kommunikasjonens innhold. Også *KRIPOS* mener at dersom det skal tas hensyn til dette argumentet, må dette være basert på en klar årsakssammenheng.

ICJ-Norge uttaler:

«Følelsen av å være overvåket – ved at slike opplysninger kontinuerlig registreres og lagres – virker dokumentert hemmende på mange. I Tyskland ble det publisert en undersøkelse som bekreftet at betydelige andeler av referansegruppen endret adferdsmønster i sin bruk av elektronisk kommunikasjon, etter at DLD var innført».

Forbrukerrådet uttaler:

«Under kapittel 4.8 om lagringstid, gjøres det på side 41 et poeng ut av den (mulige) nedkjølende effekten datalagringen kan ha på borgernes vilje til åpen og fri kommunikasjon. Etter Forbrukerrådets [ ] er denne effekten mer enn en mulighet, og kan ikke overvurderes».

NAV påpeker, i tilknytning til argumentet om datalagringens mulige nedkjølende effekt på kommunikasjon, at en del av deres brukere vegrer seg for å oppsøke NAV-kontorer. Etaten er bekymret for at datalagring kan føre til at disse også vil vegre seg mot å kontakte NAV telefonisk eller via nettet. Dette kan få utilsiktede negative konsekvenser for disse borgerne. *NAV* viser også til at de har spesialnumre til bruk for trusselutsatte, og påpeker at skjerming av data knyttet til disse spesialnumrene er svært viktig.

Faren for formålsglidning, dvs. ønske om å bruke de lagrede opplysningene til andre formål enn hva som var det opprinnelige formålet med innsamlingen, er en problemstilling som mange høringsinstanser har påpekt. Erfaring viser at det over tid er en tendens til å bruke innsamlede personopplysninger til andre formål enn innsamlingsformålet. *Datatilsynet, Norsk Presseforbund, NRK, Universitetet i Bergen, Senterungdommen, Fagforbundet Lillehammer, FriBit, Folkets høringsuttalelse, Norges Juristforbund privat, Advokatforeningen, Stopp DLD, Norsk Målungdom, ICJ Norge, Elektronisk Forpost Norge* og *Partiet Rødt* er alle bekymret for at slik formålsglidning vil kunne finne sted også for så vidt gjelder lagrede trafikkdata. Høringsinstansene viser blant annet til at det i Storbritannia er svært mange offentlige etater som har tilgang til lagrede trafikkdata for bruk til helt andre formål enn etterforskning av alvorlig kriminalitet. Flere av høringsinstansene viser også til at det er personvernutfordringer knyttet til å gi private parter tilgang til trafikkdata, for eksempel i forbindelse med avdekking av ulovlig fildeling på nett, da også dette vil kunne innebære at opplysningene brukes til annet enn bekjempelse av alvorlig kriminalitet.

Datatilsynet uttaler:

> «Selv om det er sagt uttrykkelig, både i direktivet og i departementenes utredning, at formålet med datalagringen er å avdekke, etterforske og straffeforfølge alvorlig kriminalitet, må det tas høyde for at dette utgangspunktet vil bli kraftig utfordret. Det er ingen naturlov som skal etableres.
>
> Ut fra den tanke at «det er meningsløst ikke å benytte opplysninger som allerede eksisterer», er det tilsynets erfaring at terskelen for å tillate at opplysninger som er samlet inn for ett formål også brukes til andre formål er svært lav. Tilsynet vil for eksempel minne om at ligningsmyndighetene har fått lovhjemlet adgang til opplysninger fra bompengeselskapene, til tross for at disse var lagret for det formål å fakturere bileiere som passerte bomringen. Tilsynet vil også peke på at EURODAC, som ble opprettet med det formål å identifisere asylsøkere, har blitt tatt i bruk også for politiformål (etterforskning).
>
> De gode formålene, hvor nettopp denne type opplysninger kan være betydningsfulle, står i kø. Det er nok her å nevne forskningsformål og offentlige kontrollformål (for eksempel lignings- og tollmyndigheter), og ikke minst forebygging og etterforskning av andre typer kriminalitet enn det som er foreslått pr i dag (lavere terskel). Datatilsynet er derfor overbevist om at det vil finne sted en såkalt formålsglidning, dersom datalagringen først implementeres.
>
> Det er ikke gitt at disse fremtidige endringene isolert sett vil være store. Samlet sett vil utviklingen likevel kunne være dramatisk.
>
> En formålsglidning vil kunne medføre at opplysningene spres i samfunnet på en helt annen måte enn forutsatt. Det er derfor nødvendig å ta høyde for formålsglidningen, når man skal identifisere hvilke konsekvenser datalagringen vil kunne få for personvernet på sikt.
>
> Datatilsynet kan ikke se at departementene har tatt tilstrekkelig høyde for en slik utvikling».

Advokatforeningen uttaler:

> «Det er en kjent sak at informasjon som eksisterer gjerne vil bli brukt i en helt annen sammenheng enn hva man først tenkte seg. Derfor er det nødvendig å se på direktivets konsekvenser i andre sammenhenger enn hva direktivet selv gir grunnlag for. Det er uttalt kritikk mot direktivet nettopp fordi man frykter at det vil bli åpnet for nye måter å bruke opplysningene på – alt etter hva myndighetene finner «nødvendig». Direktivet åpner således for en prinsipiell aksept av en generell «screening» av hele befolkningens dagligdagse gjøremål som på sikt kan medføre at personvernet innskrenkes ytterligere».

6.4 Departementets vurdering

Lagringsplikt for trafikkdata fra elektronisk kommunikasjon reiser mange grunnleggende personvernspørsmål. Departementet har merket seg de bekymringene høringsinstansene peker på, og er opptatt av at personvernet skal ivaretas på best mulig måte ved innføring av lagringsplikt.

Det grunnleggende nye ved implementering av datalagringsdirektivet i forhold til det som følger av gjeldende rett, er etter departementets vurdering at det vil innføres en *lagringsplikt*, og at opplysningene skal lagres for et nytt formål, nemlig kriminalitetsbekjempelse, som er et formål den behandlingsansvarlige selv ikke har direkte interesse i. I tillegg kommer en utvidelse av lagringstiden, noe som også innebærer en endring i forhold til gjeldende rett. Konkret dreier det seg alt-

så om en plikt for tilbyderne til å lagre en stor mengde data om norske borgere for det tilfellet at noen av dem skulle begå en straffbar handling, slik at dataene *kan* være av interesse for politiet i arbeidet med oppklaring av denne handlingen. I Norge har vi ikke mye erfaring med å pålegge behandlingsansvarlige å lagre personopplysninger med grunnlag i at utenforstående tredjeparter muligens kan få bruk for dem en gang i fremtiden. Innføring av datalagringsregler innebærer derfor et betydelig skritt i retning av mer overvåking og kontroll med borgerne.

Lagring av trafikkdata utgjør et inngrep i borgernes personvern. Inngrepet må sees i sammenheng med andre overvåkings- og kontrolltiltak som iverksettes. Datalagring innebærer en registrering med betydelig potensial for kontroll, noe som er en personvernutfordring. Denne ulempen må vurderes opp mot nødvendigheten og forholdsmessigheten ved tiltaket, se kapitlene 3 og 5. Etter departementets vurdering må lagringsplikten følges av regler som reduserer personvernulempen for den enkelte så mye som mulig. Blant annet vil strenge krav til sikkerhetsrutiner hos tilbyderne, god sikkerhet ved overføring av data til politiet, samt strenge regler for politiets tilgang til data, være av avgjørende betydning for å begrense personvernulempene. Konkrete tiltak blir nærmere vurdert i kapitlene 11 og 12.

Departementet er enig med *Barneombudet* i at barn har rett til et godt oppvekstmiljø, og i størst mulig grad skal ha frihet fra overvåking av ulike slag. Vi må likevel erkjenne at elektronisk kommunikasjon, og da særlig bruk av Internett, kan åpne for alvorlige krenkelser av barns integritet. Disse krenkelsene har samfunnet plikt til å beskytte barna mot. Lagring av kommunikasjonsdata som muliggjør etterforskning av nettrelatert kriminalitet, er ett tiltak i denne sammenheng. I noen sammenhenger er de elektroniske sporene politiets viktigste spor i etterforskningen. Det er derfor departementets vurdering at datalagringens positive betydning for oppklaring av en rekke alvorlige nettrelaterte krenkelser mot barn, så som tilvirkning og spredning av barnepornografi, veier tyngre enn den ulempen datalagringen representerer for barna.

Datalagring har blitt anført som nødvendig for å sikre personvern for ofre for kriminalitet. Departementet påpeker at til tross for at kriminalitet begått ved hjelp av elektronisk kommunikasjon er økende, er det fremdeles et relativt sett lavt antall kriminelle handlinger som krenker noens *personvern*. Innføring av datalagringsplikt kan derfor ikke begrunnes i ivaretakelse av ofrenes personvern som sådan, men må i stedet begrunnes i samfunnets ønske om oppklaring av flest mulig straffbare handlinger generelt.

Departementet har vurdert påstanden om at datalagring vil kunne ha en nedkjølende effekt på borgernes kommunikasjon. Det er grunn til å anta at borgere som opplever eller mistenker at deres kommunikasjon underlegges kontroll, vil være varsomme i sin kommunikasjon både av hensyn til seg selv og sine kommunikasjonspartnere. Departementet finner grunn til å understreke at det ikke er aktuelt å lagre data om kommunikasjonens innhold, men kun trafikk- og lokaliseringsdata. Departementet utelukker likevel ikke at massiv lagring av trafikk- og lokaliseringsdata over tid vil kunne påvirke frimodigheten, selv om hovedmengden av dataene aldri vil bli kontrollert eller brukt i noen sammenheng. Det foreligger per i dag imidlertid lite dokumentasjon eller empiri som kan underbygge denne påstanden. *NorSIS* viser likevel i sin høringsuttalelse til en undersøkelse om temaet gjennomført av det tyske analysebyrået *forsa Gesellschaft für Sozialforschung und statistische Analysen mbH* i 2008. I undersøkelsen kommer det frem at 11 % allerede har latt være å bruke telefon til noen typer samtaler, og 52 % mener at de antagelig ikke kommer til å bruke telekommunikasjon for å komme i kontakt med for eksempel narkotikarådgiver, psykoterapeut eller ekteskapsrådgiver. Med grunnlag i denne begrensede dokumentasjonen, finner departementet ikke å kunne legge avgjørende vekt på innvendingen om at datalagring kan ha nedkjølende effekt på borgernes kommunikasjon.

For så vidt gjelder enkelte innvendinger om at borgerne vil kunne vegre seg mot å kontakte offentlige etater når de vet at trafikkdata om kommunikasjonen lagres, er departementet opptatt av at det etableres rutiner som sørger for at kommunikasjon til gitte spesialnumre, undergis tilstrekkelig sikkerhet og ivaretar nødvendig konfidensialitet. Dette kan være samtaler til krisetelefoner, spesielle hjelpetjenester eller samtaler til offentlige etater som det kan oppleves stigmatiserende å kontakte, jf. merknader fra NAV. Det samme kan gjelde oppringninger fra brukere med avtalebasert hemmelig nummer. Det er viktig at borgerne opplever trygghet når de benytter hjelpetjenester samfunnet har etablert for dem. Allerede i dag er det slik at opplysninger om kommunikasjon til denne type tjenester lagres hos tilbyder av elektronisk kommunikasjon for fakturerings- og administrasjonsformål. Departementet er ikke kjent med at denne lagringen har representert noe problem i forhold til borgernes vilje til å

bruke disse tjenestene. Ved pålegg om lagring av dataene over lengre tid, blir det imidlertid viktig å påse at de er tilstrekkelig sikret mot uautorisert innsyn og bruk. Dette gjelder imidlertid for alle data som skal lagres, og utgjør ikke noen særskilt problemstilling for samtaler til eller fra skjermingsverdige numre. Departementet legger derfor til grunn at all data som lagres i medhold av de nye reglene, skal sikres på en måte som gjør at de kun er tilgjengelig for autorisert personell hos tilbyderen når det foreligger tjenstlig behov, og for politiet når det foreligger hjemmel for tilgang til data.

Sentralt i personvernsammenheng står prinsippet om at innsamlede personopplysninger ikke uten lovhjemmel eller samtykke fra den registrerte kan brukes til andre formål enn innsamlingsformålet. Når opplysningene først er samlet inn, viser erfaring over tid at innsamlede opplysninger likevel ofte blir benyttet til andre formål. Nye brukergrupper ønsker tilgang til data for bruk til nye formål. Dette omtales ofte som *formålsglidning*. Særlig tydelig er utfordringen i helsesektoren, der informasjon innsamlet i behandlingsøyemed, stadig oftere benyttes i forskningssammenheng, også uten at de registrerte er informert eller har samtykket. Jo mer beskyttelsesverdige de innsamlede opplysningene er, jo viktigere er det å forhindre slik formålsglidning. Data fra elektronisk kommunikasjon vurderes å være meget beskyttelsesverdig informasjon, selv om opplysningene som sådan som hovedregel ikke vil falle inn under noen av de opplysningskategoriene som personopplysningsloven definerer som sensitive personopplysninger.

Departementet mener det er viktig å fastsette klare rammer for bruken av de lagrede dataene. Hovedregelen skal være at dataene ikke kan benyttes til andre formål enn bekjempelse og oppklaring av alvorlig kriminalitet, slik dette nå nedfelles i straffeprosessloven innenfor rammene av datalagringsdirektivet. Det er et klart mål å forhindre at data gjøres tilgjengelig for andre brukergrupper enn politiet og for bruk til andre formål enn kriminalitetsbekjempelse. Ikke minst er dette viktig for borgernes tillit til myndighetene når myndighetene velger å innføre så inngripende kontrolltiltak som datalagring representerer. Departementet går derfor ikke inn for å åpne for forskriftsregulering av annen bruk av dataene. For å redusere faren for formålsglidning, mener departementet at bruk av data fra elektronisk kommunikasjon til nye formål skal besluttes av Stortinget gjennom lovvedtak. Av hensyn til internasjonale forpliktelser er det imidlertid foreslått tilgang til lagringspliktige trafikkdata også for Finanstilsynet jf. kapittel 14.5.2.

7 Hvem skal lagre

7.1 Gjeldende rett

Lagring av data fremkommet ved bruk av elektronisk kommunikasjon er som nevnt ikke noe nytt. Allerede i dag behandler, herunder lagrer, tilbydere av offentlig elektronisk kommunikasjonstjeneste eller offentlig elektronisk kommunikasjonsnett, trafikkdata for fakturerings- eller kommunikasjonsformål i en periode som er noe kortere enn datalagringsdirektivets minimums lagringstid. Det er ekomlovens definisjon av tilbydere av ekomnett og -tjenester som legges til grunn for hvem som foretar slik lagring. 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 (se kapittel 12.1 for mer om dagens regler for politiets tilgang).

Ekomlovens tilbyderbegrep er foreslått videreført i den pågående revisjonen av loven. Det gjøres imidlertid oppmerksom på at det er foreslått enkelte endringer i lovens virkeområde. Disse endringene kan, dersom de blir vedtatt, få konsekvenser for hvem som vil kunne omfattes av lagringsplikten.

7.2 Høringsnotatets forslag

Det fremgår av datalagringsdirektivets artikkel 1 at det er tilbyder av offentlig elektronisk kommunikasjonstjeneste eller offentlig elektronisk kommunikasjonsnett som skal lagre. I høringsbrevet ble det foreslått at det er ekomlovens definisjon av tilbydere av ekomnett og -tjenester som skal legges til grunn for hvem som skal lagre. 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 8.5 (opplistingen).

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, jf. § 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 tilbyderbegrepet. Andre eksempler på virksomheter som normalt faller utenfor dette tilbyderbegrepet er bedrifter, sykehus, hoteller, kafeer og lignende som utelukkende stiller elektroniske kommunikasjonstjenester til rådighet for sine kunder eller ansatte. Det vil være myndigheten etter ekomloven som i de enkelte grensetilfeller avgjør om det er snakk om en offentlig tjeneste.

Departementene foreslo i høringen at gjeldende hjemmel for myndigheten til å gi forskrift om tilretteleggingsplikt, herunder plikt til å lagre trafikkdata, videreføres 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. 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 kan det være behov for å gjøre unntak ved enkeltvedtak.

7.3 Høringsinstansens syn

Blant andre *Post- og teletilsynet, Det nasjonale statsadvokatembetet (NAST)*, *Telenor, NTV, og NHO* har kommentert forholdet hvem som skal lagre. Det er ingen høringsinstanser som har stilt spørsmål ved forslaget om å legge ekomlovens definisjon av tilbyder til grunn når det gjelder datalagringsplikten. *Post- og teletilsynet* er enig med departementene i at direktivets bestemmelser om

hvem som skal omfattes sammenfaller med ekomlovens virkeområde. Tilsynet sier videre at anvendelsen av disse begrepene vil være gjenstand for konkrete vurderinger, noe som er tilfellet i gjeldende ekomlov. *Post- og teletilsynet* støtter departementenes forslag om at det bør gis adgang til å gi bestemmelsen utvidende anvendelse gjennom forskrift eller enkeltvedtak, og at det gis dispensasjonsadgang fra lagringsplikten. Også instanser fra politisiden synes å mene det vil være hensiktsmessig å legge ekomlovens definisjon av tilbyder til grunn.

NAST fremholder at den saklige avgrensningen av lagringsplikten som følger av at den knyttes til tilbyderbegrepet i ekomloven § 1-5 nr 14, synes å være hensiktsmessig, selv om det utelukker lagring for en rekke praktiske tjenester som webmail og internettkafeer. *NAST* støtter departementenes forslag om konkrete vurderinger, og adgang til å utvide anvendelsen gjennom forskrift eller enkeltvedtak.

Det har blitt påpekt av blant andre *Telenor* at av hensyn til forutberegneligheten for tilbyderne må enhver tvil om hvem som omfattes av lagringsplikten fjernes. *Telenor* uttaler:

> «Departementene påpeker at det i noen tilfeller kan være usikkert om enkelte tilbydere eller andre aktører innenfor området vil være omfattet av lagringsplikten. Telenor mener at det er ytterst viktig at enhver slik tvil fjernes, både av hensyn til forutberegnelighet for aktørene og for å sikre like konkurransevilkår.»

Forslaget om at det i forskrift eller enkeltvedtak kan pålegges en lagringsplikt overfor andre enn de som faller inn under tilbyder begrepet støttes av Telenor. *NTV* mener at hjemmelen til å pålegge andre enn de som omfattes av tilbyderbegrepet en lagringsplikt er for tøyelig og åpner for vidtgående for at andre kan pålegges lagringsforpliktelse. *NTV* mener at det må fastsette klare grenser i lovverket for en eventuell utvidelse av pliktsubjekt. Også *NHO* reiser spørsmålet ved den foreslåtte hjemmel som gir myndighetene anledning til å pålegge andre lagringsplikt. *NHO* er bekymret for om hjemmelen vil kunne berøre norsk reiseliv (hoteller og serveringssteder) på en måte som tilsier at bransjen først må høres. Næringen besitter ikke en kompetanse til å kunne tilpasse seg et utvidet tilbyderbegrep.

7.4 Departementets vurdering

Departementet mener det er hensiktsmessig å legge ekomlovens definisjon av tilbyder av offentlig elektronisk kommunikasjonstjeneste eller offentlig elektronisk kommunikasjonsnett til grunn for å avgjøre hvem som skal omfattes av lagringsplikten. Hvem som har lagringsplikt vil da være gjenstand for konkrete vurderinger på lik linje med øvrig regulering innenfor ekomsektoren. Å foreta konkrete vurderinger av hvem som har lagringsplikt er også i tråd med anbefalingene fra EUs ekspertgruppe. Både høringsinstanser fra ekomsiden og politisiden peker på betydningen av at myndigheten gis kompetanse til å utvide anvendelsen gjennom forskrift eller enkeltvedtak. Det er departementets oppfatning at man i enkelttilfeller også skal kunne unnta tilbydere fra lagringsplikt, dersom lagring hos denne tilbyderen ikke er nødvendig for å oppnå formålet med lagringsplikten.

Datalagring på Svalbard

EØS-avtalen gjelder ikke på Svalbard. Det er derfor ikke nødvendig å gjennomføre datalagringsplikt på Svalbard av hensyn til direktivet. Ekomnettets oppbygging i dag gjør at all trafikk gjennom de norske tilbydernes nett i all hovedsak vil bli lagret på fastlandet selv om det gjøres unntak for Svalbard. Nettets tekniske oppbygning hos andre lands tilbydere på Svalbard vil sannsynligvis gjøre det vanskelig å få gjennomført en lagringsplikt for disse. Det vises blant annet til at svitsjingen for mobilnettet i Barentsburg må antas å finne sted i Russland. Det foreslås å gjøre en endring i forskrift 4. juli 2003 nr. 882 om stedlig virkeområde for lov om elektronisk kommunikasjon vedrørende Svalbard, Jan Mayen, Bilandene og Antarktis slik at lagringsplikten ikke skal gjelde på Svalbard. Dersom praksis skulle vise at dette er uhensiktsmessig, vil forskriften endres tilbake med den virkning at datalagring gjøres gjeldende på Svalbard. Kongen kan endre forskriften.

7.5 Nærmere om lovforslaget

Det foreslås at plikten til å lagre data etter ekomloven § 2-7a skal påhvile tilbyder av elektronisk kommunikasjonsnett som anvendes til offentlig elektronisk kommunikasjonstjeneste og tilbyder av slik tjeneste. Det foreslås videre en hjemmel for myndigheten til å treffe vedtak om helt eller delvis å frita fra lagringsplikten og til å pålegge andre denne plikten, dersom dette skal til for å oppnå formålet med bestemmelsen.

8 Hva skal lagres

Det fremgår av datalagringsdirektivets artikkel 5 hvilke kategorier av data som skal lagres. Departementets forslag til lovendring vil medføre innføring av lagringsplikt for trafikkdata, lokaliseringsdata og abonnements-/brukerdata som fremkommer ved bruk av elektronisk kommunikasjon som fasttelefoni, mobiltelefoni, internettaksess, e-post og bredbåndstelefoni.

8.1 Gjeldende rett

I dag lagres trafikkdata, lokaliseringsdata og abonnements-/brukerdata med hjemmel i personopplysningsloven § 31, fjerde ledd jf. personopplysningsforskriften § 71. Det er Datatilsynet som gir tilbyderne konsesjon til å behandle personopplysninger om abonnenters bruk av ekomtjenester. Formålet med behandlingen er kundeadministrasjon, opplysningstjeneste, fakturering og gjennomføring av tjenester i forbindelse med abonnentens bruk av elektroniske kommunikasjonsnett, 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 opplysningene 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 faktureringsformål. 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.

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.

8.2 Høringsnotatets forslag

I høringsnotatet ble det foreslått å stille krav om lagring av trafikkdata, lokaliseringsdata og abonnements-/brukerdata som fremkommer ved bruk av elektronisk kommunikasjon som fasttelefon, mobiltelefon, internettaksess, e-post og bredbåndstelefoni. Innhold eller noe som avslører innholdet i kommunikasjonen skal i henhold til direktivet ikke lagres. Med begrepet «avslører innholdet» mener departementet at det ikke skal lagres data som viser eller tilkjennegir kommunikasjonens innhold. Eksempler på dette er om en bruker surfer på en gitt webside, innholdet i en mulitimediamelding eller tekstmelding, eller innholdet i en e-post. Tilgangen til en brukers IP-adresse gir i dag ikke automatisk oversikt over hvor det har vært surfet, altså innholdet på websidene som har blitt besøkt. Dersom politiet skal 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.

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 blir lagret. Et eksempel på en slik tjeneste er Skype, som i utgangspunktet er en taletjeneste, men som det også er mulig å sende mulitimediameldinger og tekstmeldinger fra. Et annet eksempel er MSN som er en chattetjeneste som omfatter tale, video og oversendelse av filer. Ved

bruk av denne type tjenester vil internettilbyderne (Internet Service Provider (ISP)) som kobler opp tjenesten lagre data om at brukeren er på nett, men ISPen har ingen mulighet til å identifisere hvilke tjenester som benyttes og hvem som kommuniserer med hvem.

8.3 Høringsinstansenes syn

Post- og teletilsynet, Politidirektoratet, Kripos, Datatilsynet, Det nasjonale statsadvokatembetet, Telenor, TDC, Tele2, NetCom, IKT-Norge, Norges Juristforbund-privat, Norsk Videogramforening, Politijuristene og Høgskolen i Gjøvik har problematisert spørsmålet om hva som skal lagres.

Svært mange av høringsinstansene mener opplistingen i høringsnotatet med forslag til hva som skal lagres er i tråd med hva som fremgår av artikkel 5 i EUs direktiv. Noen høringsinstanser som for eksempel *IKT-Norge* mener høringsnotatet i liten grad var oppklarende for hva som skal lagres. IKT-Norge sier:

> «Denne uklarheten kan ha stor betydning for hvilke omfang lagringsplikten vil gi. IKT-Norge mener denne uklarheten må presiseres langt bedre før saken legges fram til politisk behandling. I følge direktivet pålegges ekomtilbyderne å lagre data som framkommer når de utfører sin tjeneste, dvs bare de data de har tilgang til jamfør direktivets punkt 13»

Datatilsynet stiller spørsmål ved om det faktisk er mulig å lagre trafikkdata om e-post som sendes og mottas via internettbasert e-postjeneste (type g-mail), uten at det er å anse som lagring av innhold. *Datatilsynet* sier:

> «Dersom departementene er av den oppfatning at også slike e-poster uansett skal registreres, må det nødvendigvis åpnes for registrering av innholdsdata. Kommer departementene til at denne type e-post likevel må forbli uregistrert, så etableres det en enkel og stor mulighet for å omgå datalagring. Dette undergraver nødvendigheten av lagringen som sådan. Datatilsynet savner en klargjøring på dette punktet.»

Også *Kripos* nevner denne problemstillingen:

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

Flere av høringsinstansene peker på det faktum at det finnes elektroniske kommunikasjonsformer som *ikke* omfattes av artikkel 5, jf. diskusjonen om at lagring er lett å omgå. Dette må ses i sammenheng med hvem som skal lagre og konsekvenser for konkurransen i ekommarkedet.

Politidirektoratet og *Kripos* peker på uklarheter i opplistingen av hva som skal lagres, og da særlig knyttet til IP-telefoni. *Kripos* sier:

> «En presisering av lagringsplikten knyttet til de ulike kategorier av IP-telefoni vil være nødvendig blant annet for å klargjøre hvem som skal lagre hvilke opplysninger.»

Høringsinstanser som *Telenor* og *Tele2* mener det knytter seg betydelig usikkerhet til hvordan en rekke krav skal forstås, og departementene oppfordres til å klargjøre og spesifisere blant annet i forskrift. *Telenor* sier:

> «Høringsnotatet opplister på overordnet nivå hvilke data som skal lagres, men det knytter seg betydelig usikkerhet til hvordan en rekke enkeltpunkter er å forstå i praksis. Telenor vil oppfordre til forutsigbarhet for tilbyderne gjennom nærmere spesifisering av kravene i forskriftsform, alternativt at det i forbindelse med Stortingets behandling av saken gis klare konkrete føringer for lagring.»

Tele2 sier:

> «I punkt 4.4.1 og punkt 4.4.2 fremgår det at A, B og C nummer skal lagres. Tele2 lagrer i dag kun trafikkdata knyttet til utgående trafikk, fordi det er dette Tele2 behøver å fakturere våre kunder. For Tele2 er det uklart om forslaget til departementet innebærer at teletilbyderne nå blir pålagt også å lagre innkommende trafikk. I så fall innebærer forslaget en vesentlig økning av informasjon som skal lagres, sammenlignet med praksis i dag.»

Videre peker enkelte tilbydere på at ikke alt som er foreslått lagret vil være enkelt tilgjengelig for tilbyder til å kunne lagre. *Telenor* sier:

> «Ikke alt som er foreslått lagret er enkelt tilgjengelig for en tjenestetilbyder selv om data-

> ene skulle finnes tilgjengelig i begrensede tidsrom i tilbyderens tekniske systemer. Dette kan være data som kun behandles for operative formål og dermed på et annet nivå enn det tilbydernes egne støttesystemer normalt behandler. I tillegg er det på flere områder uklart hva som omfattes av lagringsplikten, og dette gjør det vanskelig å forutsi om det er mulig og økonomisk forsvarlig å fremskaffe og lagre dataene.»

Tilbyderne mener myndighetene må avgrense lagringsplikten til data som er *lett* tilgjengelige for tilbyder. De forutsetter videre at direktivkrav som fremstår som uforholdsmessige og ubegrunnet i forhold til formålet ikke implementeres, for eksempel data om mislykkede oppringninger.

Flere høringsinstanser, som for eksempel *IKT-Norge* og *TDC,* gjør oppmerksom på at kvaliteten på data er varierende, og forutsetter at det ikke må iverksettes tiltak for å endre dette. *TDC* skriver:

> «TDC anbefaler videre at det klargjøres hvilket ansvar teleoperatørene har for kvaliteten på lagrede data. Hvem som kan stilles til ansvar for eksempelvis falske, manipulerte eller feil data.»

8.4 Departementets vurdering

Den prinsipielle nyskapningen med direktivet er at det innføres en plikt til å lagre data og at dette skjer for å imøtekomme myndighetenes behov. I praksis er det også en betydelig utvidelse av mengde og typer data som vil bli lagret. Opplistingen nedenfor, som med mindre endringer tilsvarer den som ble sendt på høring, gjenspeiler direktivet, og det er disse dataene som i henhold til forslaget skal lagres. Opplistingen er, som blant annet Telenor peker på, overordnet, og departementet vil derfor etterkomme ønsket fra høringsinstanser som har gitt uttrykk for behovet for en forskrift som presiserer og utdyper hva som skal lagres. En forskrift vil også kunne gi regler om leveringstid og kvalitet.

Departementet er kjent med at det finnes flere muligheter for å unngå lagring av data ved bruk av elektronisk kommunikasjon. Ved benyttelse av applikasjoner som ikke er definert som offentlige ekomtjenester vil data i tilknytning til kommunikasjonen ikke bli lagret. Eksempler på dette er sosiale nettverk og bruk av web-baserte e-posttjenester (for mer om web-basert e-posttjeneste, se kapittel 10 om konkurransen innenfor elektronisk kommunikasjon). Det finnes også ulike anonymiseringstjenester. Motstandere av datalagringsdirektivet har gjerne pekt på at innføring av en lagringsplikt er uforholdsmessig fordi det rammer alle brukere av tradisjonell elektronisk kommunikasjon, mens de som virkelig har noe å skjule kan benytte tjenester som blant annet sosiale nettverk tilbyr, og unngå lagring. Departementet er av den oppfatning at selv om det er fullt mulig å benytte elektronisk kommunikasjon som ikke lagres, kan ikke det være et tungtveiende argument for å la være å innføre en lagringsplikt på offentlig elektronisk kommunikasjonstjeneste. Det vises til kapitel 5.3.5 om behovet for nye virkemidler for oppklaring av kriminalitet.

På bakgrunn av innspill fra høringsrunden mener departementet det er nødvendig med enkelte utdypninger og presiseringer av hva som skal lagres. Dette gjelder særlig spørsmålet om lagring knyttet til bruk av IP-telefoni eller bredbåndstelefoni (ekommyndigheten benytter sistnevnte begrep).

8.4.1 Om lagring og bredbåndstelefoni

For avklaring av hva som skal lagres når det gjelder bredbåndstelefoni vises det til rapporten *«Regulering av bredbåndstelefoni etter lov om elektronisk kommunikasjon»* av 14. juni 2006, utarbeidet av Post- og teletilsynet. I rapporten oppstilles tre hovedkategorier av bredbåndstelefoni. Kategori 1 er bredbåndstelefoniløsninger som ikke er tilrettelagt for alle-til-alle kommunikasjon. Det vil si at det ikke er mulig å anrope en bruker av tradisjonelle telefontjenester via slike løsninger, men kun å kontakte et begrenset antall brukere av tilsvarende bredbåndstelefoniløsninger. Ett eksempel på bredbåndstelefoni av kategori 1 er basisversjonen av Skype. Kategori 2 er bredbåndstelefoniløsninger som delvis er tilrettelagt for alle-til-alle kommunikasjon. Dette innebærer at det er mulig enten å motta samtaler fra brukere av tradisjonelle telefontjenester, eller å anrope slike brukere. Det er imidlertid ikke mulig både å anrope og å motta anrop fra brukere av slike tjenester. Ett eksempel på bredbåndstelefoniløsninger av kategori 2 er SkypeOut, som gjør det mulig å anrope brukere av tradisjonelle telefontjenester, men ikke å motta samtaler fra slike. Kategori 3 er bredbåndstelefoniløsninger som er tilrettelagt for alle-til-alle kommunikasjon. Det vil si at det er mulig både å motta samtaler og anrope brukere av tradisjonelle telefontjenester.

Post- og teletilsynet konkluderer i sin rapport med at når det gjelder kategori 1 må det vurderes konkret i forhold til den enkelte tjeneste om det er en elektronisk kommunikasjonstjeneste eller ikke. Når det gjelder kategori 2 er denne type tjeneste å anse som en elektronisk kommunikasjonstjeneste, og forutsatt at de er tilgjengelige for allmennheten eller beregnet til bruk for allmennheten, anses de for offentlig elektronisk kommunikasjonstjeneste. Ekomregelverkets bestemmelser om elektronisk kommunikasjonstjeneste og offentlig elektronisk kommunikasjonstjeneste får anvendelse. Når det gjelder kategori 3 er denne type tjeneste en elektronisk kommunikasjonstjeneste som anses som offentlig elektronisk kommunikasjonstjeneste, og en tjeneste som anses som en telefontjeneste i henhold til ekomloven. Dersom tjenesten er tilgjengelig for allmennheten eller beregnet til bruk for allmennheten, er den å anse som en offentlig telefontjeneste. Samtlige av ekomlovens og tilhørende forskrifters bestemmelser som relaterer seg til henholdsvis elektronisk kommunikasjonstjeneste, offentlige elektroniske kommunikasjonstjenester og offentlig telefontjeneste får anvendelse.

I henhold til datalagringsdirektivet er det tilbyder av *offentlig elektronisk kommunikasjonstjeneste* og *offentlig elektronisk kommunikasjonsnett* som skal lagre data. Dette innebærer at dersom man skal følge dagens regulatoriske praksis i Norge, er det innenfor området bredbåndstelefoni tilbydere av bredbåndstelefoniløsninger av kategori 2, dersom det tilbys en tjeneste for allmennheten, og tilbydere av bredbåndstelefoniløsninger av kategori 3 som omfattes av lagringsplikten. Tilbydere av bredbåndstelefoniløsninger av kategori 1 vil kunne omfattes på bakgrunn av en konkret vurdering av Post- og teletilsynet. For mer om hvem som skal lagre og tilbyderbegrepet vises det til kapittel 7.

8.4.2 Om tilgjengelighet til data i nett og systemer

Departementet er av den oppfatning at direktivet ikke åpner for noen gradering når det gjelder hvor lett tilgjengelige dataene skal være for tilbyderne for at de skal lagres. Strengt tatt kan man si at enten fremkommer data når tjenesten produseres, eller så gjør de det ikke, og at data som fremkommer i nett og systemer skal lagres dersom det følger av direktivet. Dette er en forenkling som ikke kan gjøres ved innføring av regler om datalagring. Det vil alltid være *mulig* å hente frem data, spørsmålet er hvor langt tilbyderne skal strekke seg for å få det til. Dette vil være et ressursspørsmål. Å skulle etablere systemer for å hente ut absolutt alle data som er vanskelig tilgjengelig, vil kunne være kapasitetskrevende og ha en høy kostnad, og det må stilles spørsmål ved forholdsmessigheten i påleggene om lagring av de ulike typer data. En type data som flere høringsinstanser har reagert på at det i høringen ble fremmet forslag om lagring av, er data knyttet til mislykkede oppringninger.

8.4.3 Om mislykkede oppringninger og tapte anrop

I høringsnotatet ble det fremmet forslag om krav til å lagre data knyttet til mislykkede oppringninger og oppkoblinger. Med mislykket oppringning menes forsøk på oppringning uten at det oppnås oppkobling. Tilbyderne anser det for å være et uforholdsmessig krav å skulle lagre denne type data og mener kravet bør vurderes mer inngående. Datalagringsdirektivet er uklart når det gjelder «unsuccessful call attempts». Det fremgår av direktivet at data skal lagres dersom data genereres, eller prosesseres, lagres og logges i nettene, noe som kan tolkes som at dersom denne type data allerede lagres og logges av tilbyder, så inngår dataene i lagringsplikten. EUs ekspertgruppe har sett nærmere på dette og anbefaler følgende:

- i et nett er det bare i noen tilfeller at nettelementer konfigureres slik at de vil generere trafikkdata
- dersom slike trafikkdata genereres, vil de bli behandlet og samlet av tilbydernes systemer for oppbevaring av trafikkdata (business support systems)
- dersom denne *kombinasjonen* av generering og behandling skjer, vil dataene være omfattet av lagringsplikten

Departementet vurderer det som hensiktsmessig å legge ekspertgruppens veiledning til grunn, og er av den oppfatning at med mindre data knyttet til mislykkede oppringninger allerede i dag blir behandlet, lagret og logget, omfattes denne type data ikke av lagringsplikten.

Når det gjelder tapte anrop er departementets oppfatning at dersom de ovennevnte tre kriteriene er oppfylt, det vil si at dersom data om tapte anrop genereres og behandles vil dataene være omfattet av lagringsplikten. Kravet i datalagringsdirektivet retter seg mot oppringningsforsøk knyttet til bruk av telefonitjenester. Det presiseres i denne sammenhengen at det her er snakk om mislykkede oppringninger knyttet til taletelefoni og ikke internettaksess og e-post.

8.4.4 Om kvaliteten på de lagrede data

Datalagringsdirektivet sier ikke annet om kvaliteten på dataene enn at de skal være av samme kvalitet som de har i nettet. Departementet mener følgelig at tilbyderne ikke kan pålegges å skulle utføre kvalitetshevende tiltak på de data som de skal lagre. Et krav om økt kvalitet vil kunne føre til økte kostnader, og departementet finner ikke grunnlag for å skulle påføre tilbyderne denne type ekstrakostnader.

8.5 Nærmere om lovforslaget

Det foreslås at ekomloven § 2-7 a fastsetter hvilke kategorier av data som skal lagres, mens detaljene foreslås fremmet i en forskrift. Forskrift vil utarbeides på bakgrunn av et samarbeid mellom representanter fra politimyndigheter, representanter fra tilbydere av ekomnett og -tjenester og Post- og teletilsynet. Uklarheter i direktivet og hvordan implementering rent teknisk skal kunne skje vil kunne avklares i forskriften.

Departementet foreslår at følgende data skal lagres og at disse kan utdypes nærmere i forskrift:

Ved fasttelefoni

- 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

Ved mobiltelefoni

- 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

Ved bredbåndstelefoni

- 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 brukers kommunikasjonsutstyr eller kommunikasjonsanlegg

Ved internettaksess

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

Ved e-post

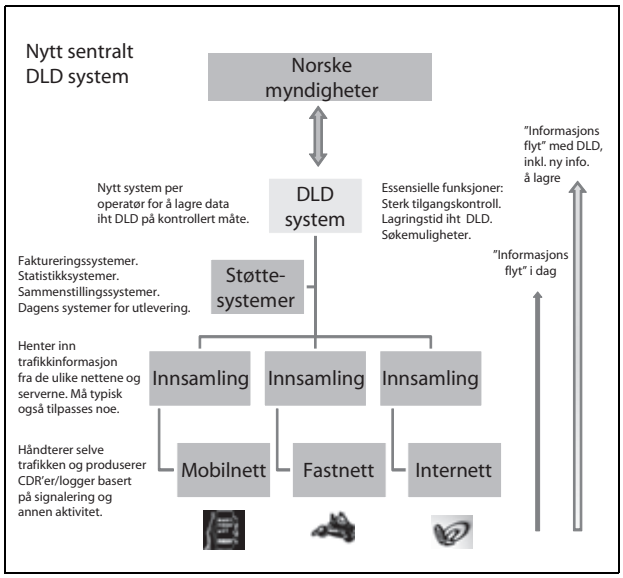
- avsender og mottakers e-postadresse og IP-adresser
- abonnentinformasjon og registrert brukerinformasjon
- dato og tidspunkt for pålogging og avlogging til e-posttjenesten

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, for eksempel ved at tilbydere av internettilgang underlegges lagringsplikt ut over den faktiske lagringen disse foretar i dag. Det er viktig å presisere at innhold ikke skal lagres. Flere detaljer om hva som inngår i de ulike momentene listet ovenfor vil fremgå i forskrift.

På bakgrunn av innspill i høringsrunden ser departementet det som viktig å presisere at alle tilbydere ikke skal lagre alt som fremgår av opp-

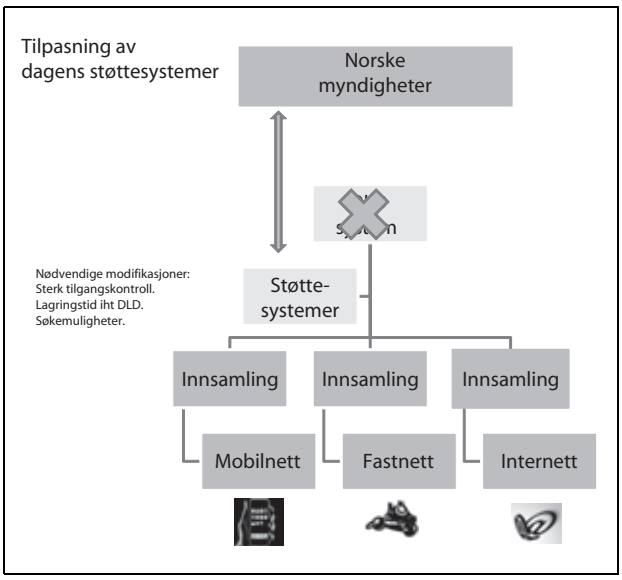
listingen. For eksempel skal den enkelte tilbyder ikke lagre alle abonnementsopplysninger knyttet til en samtale. Den enkelte tilbyder skal kun lagre data om sine *egne* abonnenter og forutsette at data om andre tilbyderes abonnenter blir lagret av de tilbyderne der hvor abonnenter hører hjemme. Dette vil etter departementets syn være i tråd med datalagringsdirektivets fortale punkt 13, som sier at data skal lagres på en slik måte at man unngår at de blir lagret mer enn én gang. Lagrings*plikten* knyttet til abonnementsdata vil gjelde for tilbyders egne kunder. Det kan i praksis være vanskelig å unngå dobbeltlagring av data all den tid verdikjeden for produksjon av ekomtjenester er kompleks. Man vil kunne oppleve at enkelte data vil være tilgjengelig flere steder hos en tilbyder i visse perioder og hos flere tilbydere samtidig. Dette vil avhenge av hvordan tilbyder finner det mest hensiktsmessig å etablere lagrings- og uthentingssystemene sine.

Som det fremgår av kapittel 11 foreslår departementet at det skal være opp til den enkelte tilbyder å avgjøre hvor og hvordan lagring og uthenting skal utføres. Figur 8.1 og 8.2 viser to eksempler på hvordan informasjonsflyten kan foregå hos en tilbyder ved gjennomføring av datalagringsdirektivet. Med det høye antall tilbydere som er i markedet for elektronisk kommunikasjon, vil man kunne forvente ulike og tilpassede løsninger for lagring og uthenting.



Figur 8.1

Illustrasjonen viser et eksempel på hvordan informasjonsflyten hos tilbyder kan bli dersom tilbyder velger å etablere et nytt system for innsamling, lagring og uthenting av data lagret i henhold til datalagringsdirektivet. Illustrasjonen er utarbeidet av Telenor.



Figur 8.2

Illustrasjonen viser et eksempel på hvordan informasjonsflyten hos tilbyder kan bli dersom tilbyder velger å tilpasse eksisterende systemer for å oppfylle kravene i henhold til gjennomføringen av datalagringsdirektivet. Illustrasjonen er utarbeidet av Telenor.

9 Lagringstid

9.1 Gjeldende rett

Som det fremgår av kapittel 8 (hva skal lagres) oppstiller ekomloven § 2-7 annet ledd en sletteplikt for trafikkdata når disse ikke lenger er nødvendige for fakturerings- eller kommunikasjonsformål. Tilbydere lagrer i dag data til ovennevnte formål i henhold til konsesjoner gitt av Datatilsynet, jf. personopplysningsloven § 31 fjerde ledd jf. personopplysningsforskriften § 7-1. Maksimal lagringstid etter konsesjonen er fem måneder etter at de ble registrert ved kvartalsvis fakturering, og tre måneder etter at de ble registrert ved månedlig fakturering. Som det videre fremgår av kapittel 8 kan data knyttet til kundenes internettrafikk per i dag lagres i inntil tre uker.

9.2 Høringsnotatets forslag

Datalagringsdirektivet fastslår i artikkel 6 at relevante data skal lagres for en periode på mellom seks måneder og to år. Høringsnotatet inneholdt ikke noe forslag til lagringsperiode, men understrekte betydningen av at en lagringstid må balansere hensynet til kriminalitetsbekjempelse og hensynet til personvern. Hensynet til personvern tilsier at de relevante data ikke skal lagres lengre enn hva som er nødvendig av hensyn til kriminalitetsbekjempelse.

I høringsnotatet viste departementene til at hensynet til kriminalitetsbekjempelsen taler for fastsettelse av en lengre lagringsperiode enn seks måneder. Saker der det kan være spesielt behov for data eldre enn seks måneder er saker om terrorhandlinger og annen alvorlig kriminalitet, herunder saker om seksuelle overgrep, volds- og narkotikalovbrudd, organisert kriminalitet og lovbrudd med internasjonale relasjoner. Det kan være behov for lengre lagringstid enn ett år i saker der etterforskningen strekker seg over lang tid og hvor etterforskningen er tidkrevende. Det kan også gjelde der hvor nye omstendigheter dukker opp under førsteinstansbehandlingen i domstolen. Domstolenes bevisvurderinger kan være vanskelige, og i enkelte saker kan elektroniske data være avgjørende bevisstøttepunkter. Siden elektroniske data skal opplyse saken, kan de også tale til gunst for siktede. En begjæring fra forsvarer til påtalemyndigheten om å innhente (nye) data kan komme på et så sent tidspunkt i etterforskningen eller pådømmelsen at data har gått tapt.

Begrunnelsen for ikke å innføre lengre lagringstid enn seks måneder er i hovedsak personvernmessige hensyn. Det er sentralt i personvernsammenheng at personverninngrep aldri skal være større enn strengt nødvendig for formålet. En viktig innvending mot datalagring er inngrepet i borgernes kommunikasjonsfrihet. Innføring av datalagringsregler vil innebære en utvidelse av de typer data som skal lagres sammenliknet med det tilbyderne lagrer i dag. Samtidig utvides lagringstiden. Jo flere data som lagres, og jo lenger de lagres, jo større blir den akkumulerte informasjonsmengden, og jo enklere er det å analysere de registrertes kommunikasjonsmønstre, avdekke deres kontaktnett, bygge personprofiler etc. Det kan ikke utelukkes at denne muligheten for sammenstilling av data kan ha en nedkjølende effekt på borgernes kommunikasjon. Dette taler for å holde lagringstiden så kort som mulig, fordi kort lagringstid vil redusere mulighetene for kommunikasjonsanalyser og profilbygging noe. Hensynet til majoritetens personvern, tilsier at man bør velge det minst inngripende lagringsalternativet.

Norske myndigheter har innenfor elektronisk kommunikasjon en tradisjon for å se hen til de andre nordiske land når det gjelder regulering. Danmark og Finland har innført ett års lagringstid. Sverige har ennå ikke implementert datalagringsdirektivet. (Se kapittel 4.3.)

Departementene har merket seg at enkelte land skiller på lagringstid for ulike tjenester. Nederland har for eksempel ett års lagring for data knyttet til bruk av fasttelefon og mobiltelefon, og seks måneders lagring for data knyttet til bruk av Internett. I høringsnotatet fremmet departementene forslag om ikke å skille på lagringstid etter teknologi. Teknologinøytral regulering er et viktig prinsipp innenfor elektronisk kommunikasjon. Det vil si at regulering av en tjeneste skal være lik,

uavhengig av teknologi eller produksjonsmåte. Ulik lagringstid kan innebære konkurransefordeler for tilbydere av tjenester basert på en teknologi som får kortere lagringstid enn tilbydere av tjenester basert på 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. Høringsinstansene ble særskilt bedt om sitt syn på lagringstid.

9.3 Høringsinstansenes syn

Post- og teletilsynet, Politidirektoratet, Riksadvokaten, Økokrim, Oslo statsadvokatembeter, Kripos, PST, Det nasjonale statsadvokatembetet, Telenor, NetCom, Ventelo, Get, Tele2, TDC, Kabel Norge, NextGenTel, Politijuristene, Politiets felleforbund, Norsk Narkotikapolitiforening, IKT-Norge, Stine Sofie stiftelsen, UNIO, HSH, Finansnæringens Fellesorganisasjon, Akademikerne, Teknologirådet, Advokatforeningem, NITO, TEKNA, og *NorSIS* har problematisert spørsmålet om lagringstid.

Det er viktig å merke seg at en rekke av de høringsinstanser som har uttalt seg om lagringstid, ikke nødvendigvis er for implementering av direktivet. Noen sier eksplisitt at de ikke tar stilling til for eller mot. Andre, som for eksempel *IKT-Norge* og *NITO* er prinsipielt i mot, men uttaler seg subsidiært om lagringstid, og ønsker minimumstid.

Post- og teletilsynet har vurdert ulike typer saker og ulike typer tjenester opp mot lagringstid. Tilsynet mener det i mange saker kunne vært aktuelt å gi fritak fra taushetsplikten en lengre periode tilbake i tid, hvis dataene var lagret, og at dette skulle tilsi lang lagringstid. Basert på erfaringene med håndteringen av politiets fritaksbegjæringer uttaler tilsynet følgende:

> «[…], er det PTs inntrykk at politiet kun i et fåtall av tilfellene begrenser sine begjæringer om fritak fra taushetsplikten for å kunne få utlevert historiske trafikkdata til perioder som er kortere enn slike data faktisk lagres i dag. Det er også PTs inntrykk at det i mange saker ville vært aktuelt å gi fritak for en lengre periode tilbake i tid, hvis dataene var lagret. Særlig gjelder dette i narkotikasaker, hvor de mistenkte i mange tilfelle mistenkes for å ha bedrevet den kriminelle aktivitet i lengre perioder enn den perioden hvor dataene faktisk lagres i dag. Dette gjelder imidlertid ikke i alle typer saker.»

I relasjon til basestasjonssøk er det tilsynets erfaring at det veldig sjelden anmodes om å muliggjøre basestasjonssøk lengre tilbake i tid enn to måneder. Tilsynet uttaler følgende om basestasjonssøk:

> «I relasjon til å kunne foreta basestasjonssøk, er det PTs erfaring at dette sjeldent begjæres for perioder særlig langt tilbake i tid. Som oftest mottar PT begjæringer for å muliggjøre slike søk innen samme arbeidsuke som den aktuelle kriminelle handling har skjedd. Det understrekes imidlertid at det er unntak fra dette, men det er veldig sjeldent at PT mottar begjæringer for å muliggjøre basestasjonssøk lenger tilbake i tid enn to måneder. Basert på politiets nåværende bruk av basestasjonssøk som etterforskningsmetode, tilsier ikke hensynet til å kunne foreta basestasjonssøk lengre lagringstid enn direktivets minimum.»

Post- og teletilsynet foreslår etter en helhetsvurdering, og under forutsetning av det tilgangsregimet som høringsnotatet fremmet forslag om, ett års lagringstid.

De fleste høringsinstansene fra politisiden ønsker så lang lagringstid som mulig.

Politidirektoratet uttaler:

> «Med alvorlig og organisert kriminalitet ser vi en økende grad av internasjonal etterforskning, et økende fokus på bakmenn og en større grad av profesjonalitet blant kriminelle. Politidirektoratet ser det derfor slik at man som utgangspunkt ønsker at lagringstiden i direktivet utnyttes fullt ut, dvs. en lagringstid på to år.»

Likevel mener Politidirektoratet at avveid mot hensyn til personvern og kostnader kan det innføres kortere lagringstid enn to år (minst ett år).

Riksadvokaten antar at en lagringstid på ett år vil være tilstrekkelig for de behov politiet har i de fleste saker, og understreker at også seks måneders lagringstid vil være av stor betydning. *Oslo Statsadvokatembeter* peker på at økt lagringstid samler mer informasjon som kan gi større nytteverdi, og de peker på muligheten for seks måneders lagring. Seks måneders lagring vil være en begrenset økning i forhold til i dag og innebære at politiets arbeid ikke endres vesentlig. *Kripos* ønsker minst ett års lagringstid og begrunner dette med at de bedriver reaktiv etterforskning, at etterforskningen er en dynamisk prosess, at det er økt grad av profesjonalisering blant kriminelle og at etterforskning ofte har internasjonal karak-

ter. *Politiets sikkerhetstjeneste* mener lagringstiden bør være ett år på linje med de fleste europeiske land. Det samme mener *Det nasjonale statsadvokatembetet*.

Av andre høringsinstanser som foreslår ett års lagringstid, herunder *HSH* og *Finansnæringens Fellesorganisasjon*, er det særlig behovet for harmonisering med andre nordiske land som er begrunnelsen. Organisasjoner som representerer bransjer som er særlig utsatt for vinningskriminalitet ønsker harmoniserte internasjonale regler for at politiet skal få virkemidler til å etterforske denne type saker.

Samtlige tilbydere av ekomnett og -tjenester som uttaler seg om lagringstid mener det eventuelt må innføres seks måneders lagring da dette vil være minst inngripende i kundenes privatliv.

Telenor uttaler:

> «Telenor anbefaler kortest mulig lagringstid da dette er minst inngripende opp mot den enkelte kundes privatliv. Vi støtter også at lagringstid skal være teknologinøytralt, det vil si samme lagringstid for alle data.»

TDC peker på at det ikke er dokumentert behov for lengre lagringstid, mens *Kabel Norge* viser til at de fleste forespørslene fra politiet skjer i de tre første måneder av en etterforskning.

Også andre, herunder *IKT-Norge, Akademikerne, Teknologirådet* og *NorSIS* ønsker en kortest mulig lagringstid.

NorSIS uttaler:

> «NorSIS støtter departementenes oppfatning om at lagringstiden bør balansere hensyn til kriminalitetsbekjempelse og hensynet til personvern. NorSIS er av den oppfatning at man bør begynne med en restriktiv lagringstid, dvs. minimumskrav. Andre lands erfaringer bør også legges til grunn ved beslutning om lagringstid. NorSIS mener at datalagringstiden heller bør justeres på sikt enn å settes høyt i utgangspunktet».

Advokatforeningen mener at utsettelsen av spørsmålet om lagringstid splitter debatten på en beklagelig måte og at det å utelate forslag om lagringstid i høringen er sterkt kritikkverdig.

9.4 Departementets vurdering

Datalagringsdirektivet foreskriver som nevnt ovenfor at lagringstiden skal være mellom seks måneder og to år. I dette tidsspennet foreslår departement at det i Norge skal gjelde en lagringstid på ett år. Det er i samsvar med det behov som nærmest unisont har kommet fra politi og påtalemyndighet. En del andre europeiske land, herunder Danmark og Finland har også lagt seg på ett års lagringstid.

Departementet har merket seg at svært mange høringsinstanser er i mot datalagringsdirektivet og i den grad de har uttalt seg om lagringstid går inn for at den skal være kortest mulig. Det har fremkommet mange gode argumenter for å velge kort lagringstid, men en rekke momenter trekker også i retning av lengre lagringstid enn minimumstiden på seks måneder.

Post- og teletilsynets erfaringer når det gjelder begjæringer om fritak fra taushetsplikt for innhenting av trafikkdata, støtter forslaget om ett års lagringstid. Tilsynet har gjennom en årrekke opparbeidet seg kompetanse og oversikt over hvilke saker som skulle tilsi lang lagringstid og hvilke saker som skulle tilsi kort lagringstid. Når tilsynet anbefalte ett års lagringstid i sitt høringssvar, var det under forutsetning av at reglene om politiets tilgang til data skulle skjerpes. For så vidt gjelder forutsetningen ligger den også til grunn for dette forslaget, jf. kapittel 12.

Departementet mener en avveining mot personvernet ikke tilsier en lagringstid på to år. Data lagres i dag fra tre til fem måneder, og et sprang til to år vil være for stort, og kan etter departementets vurdering ikke forsvares i forhold til politiets dokumenterte behov. Informasjon om bruk av Internett lagres 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 rett. Politi og påtalemyndighet opplever at lagringsperioden på tre uker er alt for kort i saker om internettrelaterte seksuelle overgrep. Dette kommer klarest til uttrykk i saker hvor politiet får melding om et lovbrudd først etter at lagringsperioden på tre uker har utløpt. Det vises til at en del ofre bruker tid på å bearbeide hendelsen og eventuelle traumer før saken anmeldes. I tillegg kommer at saker hvor det samarbeides med utenlandske politimyndigheter er tidkrevende.

Kripos har bl.a. fremholdt at anmodninger om utlevering av data over landegrenser kan være tidkrevende, siden slike anmodninger ofte behandles av en rekke instanser. Hensynet til internasjonalt samarbeid og etterforskning taler derfor også for en noe lengre lagringstid enn direktivets minimum på seks måneder.

Foreløpige signaler fra EU tyder på at politiet i det alt vesentlige etterspør data som er nyere enn seks måneder. Etter dette går etterspørselen etter data ned, selv om det også etterspørres en del data frem til de er 12 måneder gamle. Bare unntaksvis etterspørres data eldre enn 12 måneder. Storbritannias EU-formannskap viste i forbindelse med vedtakelsesprosessen av direktivet til en britisk undersøkelse hvor det fremgår at 85 % av de data som ble brukt, var mindre enn seks måneder gamle. Undersøkelsen viste imidlertid at data som var mellom syv og tolv måneder gamle ble brukt i de alvorligste sakene, fortrinnsvis drapssaker.

Dette stemmer med norske erfaringer. Både i Orderudsaken (kapittel 5.4.7.6) og Nokassaken (kapittel 5.4.7.8) ble det etterspurt data som var eldre enn seks måneder. I Nokassaken ble det satt inn maksimalt med ressurser, men data gikk tapt fordi seks av de senere domfelte, deriblant hovedmannen, ble pågrepet etter at lagringsperioden var utløpt. I alvorlige saker kan etterforskningen være krevende fordi gjerningspersonene har vært bevisste på å dekke til spor etter forbrytelsen. Informasjon som legger et grunnlag for innhenting av data kan komme sent i etterforskningen av alvorlige saker. Et typeeksempel på tidkrevende etterforskning er saker hvor politiet må gå gjennom lister over hundrevis av alibikandidater for utsjekking, for eksempel på grunnlag av et basestasjonssøk ved åstedet, eller ved søk etter matchende DNA-materiale. Ifølge Kripos' undersøkelse (kapittel 5.4.6.3) var 50,4 % av etterforskerne i 966 saker «helt enig», og 9,5 % «litt enig» i at det ville vært aktuelt å hente trafikkdata lengre tilbake i tid dersom dette hadde vært mulig i forhold til dagens lagringspraksis. I 21,5 % av sakene var etterforskerne «helt uenige» i dette. Tallene for IP-trafikk var også noe lavere. Et par eksempler på saker hvor det ville vært aktuelt for politiet å innhente eldre data, er sakene «Operasjon Broken Lorry» og «Operasjon Andromeda», begge omtalt i kapittel 5.4.7.2. I disse sakene var norske trafikkdata slettet, men som følge av politisamarbeid fikk politiet tilgang til eldre data fra henholdsvis Nederland og Sverige, hvor lagringstiden er lengre. Saker om savnede personer som senere får status som drapssak er en annen type saker hvor kort lagringstid kan føre til at data går tapt (sakseksempel i kapittel 5.4.7.12).

Etter departementets syn taler også behovet for å bekjempe terror for ett års lagringstid. Den britiske undersøkelsen viste at i halvparten av sakene som gjaldt etterforskning av terrorhandlinger, var de etterspurte data over seks måneder gamle. Ifølge PST stemmer dette med norske erfaringer. Behovet for eldre data gjelder også andre saker som PST har ansvaret for, hvor de mistenkte gjennomgår en «bearbeidingsprosess» på forhånd. Dette kan være sosialisering inn i et ytterliggående religiøst miljø, eller personer som søkes vervet av etterretningsoffiserer.

Departementet har merket seg at de fleste tilbyderne er i mot datalagringsdirektivet og har uttrykt bekymring for kundenes personvern. Det følger av dette at tilbyderne ønsker så kort lagringstid som mulig dersom en lagringsplikt skal innføres.

Departementet har videre merket seg at tilbyderne er opptatt av kostnadene knyttet til lagring og lagringstid. Det fremgår av Telenors høringsuttalelse at kostnadene vil øke desto lengre man skal lagre data.

Departementet vil i den forbindelse vise til Teleplans utredninger som sier at lagringstid bare i noen grad virker inn på kostnadene for tilbyder. Lagringskapasitet er etter Teleplans oppfatning ikke en betydelig kostnadsdrivende faktor. For mer om kostnader, se kapittel 16. Kostnadene vil uansett ikke være avgjørende for valg av lagringstid, her vil politiets behov og hensynet til personvernet veie tyngre.

9.5 Nærmere om lovforslaget

En lovbestemt lagringsplikt vil føre til lik lagringstid hos alle tilbydere for de dataene lagringsplikten gjelder. Departementet foreslår at det innføres en lagringstid på 12 måneder for de data som fremgår av kapittel 8. Det foreslås videre at det ikke skal skilles mellom teknologier. Dette medfører at det foreslås lik lagringstid for de ulike tjenestene og ulike typer data.

10 Konkurransen innenfor elektronisk kommunikasjon

10.1 Innledning

Et viktig hensyn som må vurderes og avveies 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. Direktivet overlater 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 konsekvenser. 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 må innstille virksomheten. Departementets forslag om at tilbyderne selv kan velge lagringsløsning, åpner for at den enkelte tilbyder kan finne mest mulig hensiktsmessige, økonomisk effektive og sikre lagringsløsninger. Departementet mener samtidig det bør legges til rette for løsninger som fører til en rimelig kostnadsdeling mellom myndighetene og tilbyderne slik at kravene ikke blir urimelig tyngende for de små tilbyderne av ekomtjenester.

10.2 Høringsinstansenes syn

Post- og teletilsynet, Telenor, TDC, Ventelo, Kabel Norge, Altibox, HP, Get, Abelia, IKT-Norge og NorSIS har problematisert konkurransen innenfor elektronisk kommunikasjon.

Flere av høringsinstansene påpeker at datalagringsdirektivet ikke er konkurransenøytralt. *Post- og teletilsynet* mener det ikke er mulig å si hvorvidt konkurransen i markedet vil bli påvirket. Dette vil avhenge blant annet av kostnadene for tilbyderne.

Telenor peker på at direktivet ikke gir ønsket forutberegnelighet og konkurransevilkår for aktørene. Telenor sier videre:

> «Konkurransen om elektroniske nett, tjenester, applikasjoner og innhold skjer i stadig større grad på et internasjonalt marked. Webbaserte e-posttjenester som Gmail og Hotmail, samt peer-to-peer IP-basert tjeneste telefonitjenester som Skype, er eksempler på tjenester som norske brukere benytter seg av, der tjenestene vedlikeholdes og leveres i utlandet. Det er i den sammenheng viktig at norske myndigheter, i tilfelle direktivets innlemmelse vedtas, ikke velger å gjennomføre en svært streng og detaljert norsk implementering av datalagringsdirektivets allerede i utgangspunktet voldsomme omfang».

Abelia sier:

> «Om direktivet innføres i norsk rett, mener Abelia at det er viktig at implementeringen skjer på en konkurranse- og teknologinøytral måte. Slik forslaget nå foreligger åpnes det for en tvil om hvilke applikasjoner og aktører som er pålagt lagring, og det legges opp til at enkelte applikasjoner ikke er omfattet av lagringsplikten. Slike forskjeller vil kunne påvirke konkurranseforholdene og dessuten uthule de ønskede konsekvensene som direktivet er ment å ivareta».

TDC mener erfaringen fra EU viser at reglene for datalagring virker svekkende for konkurransen i enkelte land. *TDC* mener videre at konkurransen påvirkes fordi de små aktørene ikke vil ha tilsvarende ressurser som store aktører til å benytte til lagring og utlevering av data. Plikten vil kunne virke som en barriere for etablering, noe også *Post- og teletilsynet* nevner.

NorSIS sier:

> «Norge er et spesielt land med svært mange små bedrifter. Dette gjelder også for tilbyderne. Dersom datalagring blir kostbart for til-

byderne kan noen velge å ikke tilby de ulike tjenestene i distriktene».

De aller fleste tilbyderne og *IKT-Norge* peker på utfordringen med at plikten rammer ulike teknologier forskjellig. De tradisjonelle ekomtilbyderne må oppfylle krav som de applikasjonsbaserte leverandørene ikke må.

Telenor uttaler:

«Hvis for eksempel web-baserte tjenester ikke pålegges de samme reglene for lagring, er det ikke usannsynlig at brukere, også de som ikke har kriminelle hensikter, ønsker å flytte til de tilbyderne og de tjenestene som ikke er pålagt å lagre. For eksempel når det gjelder e-post, er det uheldig at de som tilbyr tilgang til e-post på vanlig måte, dvs via et e-postprogram på brukerens maskin, må lagre data, mens de som har et web-grensesnitt til e-posttjenesten, ikke nødvendigvis behøver å lagre».

Telenor tilbyr både web-basert eposttjeneste og tradisjonelle epostprogrammer, og vil etter datalagringsdirektivet reguleres ulikt avhengig av grensesnittet for å sende e-posten. I følge Telenor kan samme argumentasjonen benyttes om andre web-baserte tjenester.

10.3 Departementets vurdering

Departementet vil understreke viktigheten av 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 slik 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. Innføring av datalagringsdirektivet vil gi variasjoner mellom landene både når det gjelder lagringstid og kostnadsdekning, men i mindre grad enn om man ikke harmoniserer reglene.

Når det gjelder enkelte høringsinstansers påpekning av at innføring av datalagringsdirektivet vil føre til at små tilbydere vil rammes hardere enn store tilbydere, er dette en bekymring som departementet deler. Innføring av en plikt til å lagre data innebærer en kostnad. De største tilbyderne har allerede etablert enkelte systemer for lagring, det gjelder særlig tilbydere av fasttelefontjeneste og mobiltelefontjeneste. For disse tilbyderne vil en eventuell innføring av lagringsplikt medføre at de må lagre mer data og andre typer data enn de gjør i dag for kommunikasjons- og faktureringsformål. De vil måtte bygge ut de eksisterende systemene sine eller investere i nye systemer for lagring og uthenting. For små tilbydere, som per i dag ikke foretar noen lagring av data, vil innføringen av en lagringsplikt medføre at de må investere i nye lagrings- og uthentingssystemer.

Departementet har likevel tiltro til at også de små tilbyderne vil kunne klare investeringene. Utviklingen har kommet såpass langt på det europeiske markedet når det gjelder datalagring, og små tilbydere vil derfor ha mulighet til å kunne investere i relativt billige «hyllevareprodukter» for lagring. Alternativt kan det inngås avtale med andre tilbydere om lagring. Kjøp av lagringstjeneste er også mulig. Lovforslaget gir ingen begrensninger i så måte – det er helt opp til tilbyder å velge lagringsløsning, så lenge løsningen tilfredsstiller kravene til informasjonssikkerhet.

Departementet har merket seg at mange høringsinstanser mener at datalagringsdirektivet ikke er konkurransenøytralt. Det at enkelte tjenester omfattes og andre ikke, kan være en utfordring for konkurransen i markedet. Samme tjenester på ulikt format konkurrerer om de samme kundene, og det er en uheldig konsekvens av datalagringsdirektivet at tradisjonelle ekomtilbydere må lagre mens de som tilbyr applikasjonsbaserte innholdstjenester ikke må lagre. Eksemplet fra Telenor om tradisjonell e-posttjeneste versus web-basert e-posttjeneste forklarer denne utfordringen godt. Den uheldige konsekvensen følger av at datalagringsdirektivet ikke omfatter absolutt alle data knyttet til elektronisk kommunikasjon, men er avgrenset til de data som er listet opp i kapittel 8. Med mindre man ønsker at absolutt alle data skal lagres, må det settes en grense et sted, med den konsekvens at det blir en viss forskjellsbehandling. Det er for tidlig å si om denne forskjellsbehandlingen faktisk får noen konsekvenser for konkurransen, jf. høringsinnspillet fra Post- og teletilsynet.

For personvernet er det utvilsomt positivt at det ikke skal lagres data knyttet til web-basert eposttjeneste. Web-basert e-posttjeneste er etter ekomregelverket å anse som *innhold* fordi det ved bruk av slik tjeneste fremgår *hvor* man har surfet på nettet. Departementet ønsker ikke å pålegge lagringsplikt for denne typen tjenester fordi det ville være i strid med det absolutte kravet om at innhold ikke skal lagres. Dersom man i regelverket hadde stilt krav om lagring av data knyttet til web-surfing, ville også de som leverer denne typen tjenester blitt omfattet av lagringsplikten. Lagring av data om web-surfing inngår ikke i det

forslaget som nå fremmes og det skal følgelig ikke lagres data knyttet til bruk av for eksempel en hotmail-konto. Eventuelle uklarheter knyttet til hvem og hvilke tjenester som omfattes av lagringsplikten, vil kunne avhjelpes i enkeltvedtak eller forskrift.

11 Lagringssted og informasjonssikkerhet

11.1 Gjeldende rett

I dag er hver enkelt tilbyder behandlingsansvarlig etter personopplysningsloven § 2 nr. 4 for data lagret for fakturerings- og administrasjonsformål. Tilbyderen kan velge å lagre data fysisk hos seg selv, eller benytte en databehandler for ekstern lagring. Valg av lagringsløsning påvirker imidlertid ikke behandlingsansvaret, og det er tilbyderen selv som er ansvarlig for etterlevelse av personopplysningsregelverket, herunder sikring, og bruk og sletting av de lagrede dataene i henhold til gjeldende regelverk. Lagrede data skal sikres i samsvar med personopplysningsloven § 13 og personopplysningsforskriften kapittel 2 om informasjonssikkerhet.

11.2 Høringsnotatets forslag

Datalagringsdirektivet presiserer 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.

I 2006 fikk departementene utredet kostnadene knyttet til ulike lagringsmodeller, jf. kapittel 16.3. 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 som har 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 skal skje.

Departementene foreslo i høringsnotatet at data fortsatt skal lagres hos tilbyderne, og at data skal hentes ut av tilbyderne. I høringsnotatet forutsatte departementene at det settes opp egne lagringsløsninger for data som lagres for myndighetenes formål og at disse holdes atskilt fra forretningsmessige data. Det ble redegjort for lagringsløsninger hvor tilbyderne er pliktige til å overføre data til en sentral database, 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. En mellomløsning er at myndighetene etablerer en sentral database som det er frivillig for tilbyderne å knytte seg til. 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.

Ut fra personvernmessige vurderinger er det betenkelig å samle alle data på ett sted. En slik samling av store mengder personopplysninger kan i seg selv utgjøre en ekstra personvernrisiko. Selv om det vil være en forutsetning med tilstrekkelig sikkerhet for at data ikke blir brukt til andre formål enn hva som var formålet med lagringen, er det alltid en fare for utilsiktet utlevering eller misbruk, og skadepotensialet er større jo mer informasjon som er samlet på ett sted. Departementene gikk derfor i høringsnotatet ikke inn for en sentral lagringsløsning, men utelukket ikke at små tilbydere kan gå sammen om en felles lagringsløsning.

11.3 Høringsinstansenes syn

Høringsinstansene er delt i synet på lagringssted. Alle høringsinstansene står imidlertid samlet bak synspunktet om at dataene må underlegges tilfredsstillende sikring. Mange høringsinstanser peker på at det er knyttet store sikkerhetsutfordringer til at så store mengder data skal lagres og håndteres av så mange personer som datalagring etter direktivet forutsetter. Dette er en gjennomgående kommentar uavhengig av om høringsinstansen ellers går inn for lokal eller sentral lagring av data.

NTNU, Kripos, NHO, NITO, TEKNA, Norsk Narkotikapolitiforening og *Politiets fellesforbund* mener alle at lokal lagring av data hos den enkelte tilbyder vil representere en større sikkerhets-

risiko enn ett sentralt lagringssted, og går derfor inn for sentral lagring av data. Det er imidlertid ulik oppfatning blant disse om hvorvidt den sentrale databasen bør eies av staten eller av tilbyderne i fellesskap. *Kripos* påpeker at en sentralisert lagring med sanntidskryptering vil redusere de personvernmessige betenkelighetene til et absolutt minimum, og at kun ett kontaktpunkt vil innebære en betydelig ressursbesparelse for politiet ved uthenting av data og sikre raskere tilgang. *Kripos* mener at en kryptert lagringsløsning (sanntidskryptering av alle lagrede data) vil øke sikkerheten rundt de lagrede dataene i meget stor grad. Ved å velge sentral lagring vil myndighetene ha bedre mulighet til å påvirke valg av løsning slik at sikkerhetshensyn bedre kan ivaretas og tillegges større vekt enn kostnader og ordinær drift. *Kripos* er ikke enig i at lokal lagring gir bedre sikkerhet for at dataene ikke brukes til andre formål enn de er ment for, eller at det gir større sikkerhet mot utilsiktet utlevering. Tvert i mot mener *Kripos* at en sentral lagring der dataene er kryptert ivaretar disse hensynene best.

Kripos uttaler:

> «Ett lagringssted som er uavhengig av tilbyderne vil medføre en åpenbart bedre sikkerhet mot at uvedkommende får kunnskap om de etterforskningsskritt politiet har iverksatt. Lekkasje av slik informasjon kan selvsagt både skje forsettlig fra noen som ser seg tjent med det, men kan også skje uforvarende eller ved en tilfeldighet. Det kan uansett være til stor skade for etterforskningen. At 230 tilbydere skal ekspedere slike henvendelser fra politiet medfører en åpenbart større risiko for slike lekkasjer. Det finnes flere eksempler på at problemstillingen er reell».

Kripos uttaler videre:

> «Høringsnotatet støtter seg til Datatilsynets innvendig mot sentralisert lagring når det gjelder den personvernrisiko dette medfører. Dette resonnementet synes utelukkende å basere seg på skadepotensialet ved et sikkerhetsbrudd, og i liten grad sannsynligheten for selve bruddet. Skadepotensialet ved enkeltbrudd er åpenbart større om alle data lagres på ett sted.
>
> Likevel har ikke høringsnotatet drøftet denne problemstillingen opp mot en løsning med sanntidskryptering av data, se pkt. 4.1. Som nevnt tidligere er ikke en kryptert lagringsløsning omhandlet i høringsnotatet eller i de forutgående utredningene. Kripos finner dette merkelig da en kryptert løsning vil øke sikkerheten rundt de lagrede data i meget stor grad.
>
> Kripos anbefaler en kryptert lagringsløsning. Men skulle man av ukjente årsaker velge en ukryptert løsning, så er faren for at flere sikkerhetsbrudd inntreffer like åpenbart større om man overlater lagring og utlevering til et stadig økende antall tilbydere».

Også *Politidirektoratet* støtter sentral lagring fordi direktoratet mener dette vil sikre lik lagringspraksis hos alle tilbyderne, og bidra til at hensynet til personvern og annen lovgivning blir ivaretatt. Direktoratet forutsetter at det ikke er politiet selv som skal foreta lagringen.

Det nasjonale statsadvokatembetet mener datalagringens legitimitet best ivaretas ved lagring utenfor politiet, dvs. hos en av de store tilbyderne eller en uavhengig instans. De mener den sikreste ordningen vil være lagring hos én aktør fordi dette vil forenkle innhenting samtidig som sentral datalagring gir klar ansvarsplassering mht. hvem som er behandlingsansvarlig, og forenkler kontroll og tilsyn. Sentral lagring gjør det mulig å ta i bruk personvernfremmende teknologi for å beskytte alle dataene på et godt nivå. *Det nasjonale statsadvokatembetet* mener sentral lagring må antas å være enklest, rimeligst og best oppfylle formålet med datalagring, og savner en vurdering av om bruk av personvernfremmende teknologi vil styrke en slik løsning.

NAST uttaler:

> «NAST mener at datalagringens legitimitet best ivaretas ved at dataene lagres hos en aktør utenfor politiet, og lagringen må skje under så betryggende forhold som mulig. NAST antar at den sikreste og ryddigste ordningen er å lagre alle dataene hos én aktør. For politiet vil det forenkle innhenting av opplysningene. Det ligger ikke noe sikkerhetselement i at politiet som i dag, må henvende seg til forskjellige tilbydere. Det bare forsinker etterforskingen. Sentral datalagring gir klar ansvarsplassering mht. hvem som er den behandlingsansvarlige, forenkler kontroll og tilsyn med ordningen og oppfyller formålet på beste måte.
>
> Prinsipielt mener NAST at spørsmål om datasikkerheten hos tilbyderne ikke bør være noe argument ved valg av lagringssted. Som enhver annen forretningsdrivende må tilbyder behandle sine data profesjonelt og i samsvar med lovverket. Men hvis det virkelig er slik at

man må påregne at bransjen ikke kan håndtere dataene forsvarlig, styrkes jo argumentet for sentral datalagring. Det frigjør også ressurser som i dag går med hos tilbyderne til å betjene politiets utleveringsbegjæringer. Ved sentral lagring er det også mulig å ta i bruk personvernøkende *teknologi* for å beskytte *alle dataene* på et godt nivå. NAST savner en vurdering i høringsbrevet om bruk av slik teknologi ville styrke forslaget om sentral datalagring. Det må anses å være enklest, rimeligst og best oppfylle formålet med datalagring».

NAV påpeker at gruppen tilbydere er svært lite homogen, og at kanskje ikke alle vil klare å iverksette fullgode mekanismer for sikring av dataene. Mange av tilbyderne av elektroniske kommunikasjonsnett og -tjenester påpeker at tilbydere som er etablert i flere EU-/EØS-land bør ha muligheten til å samlokalisere lagring av data fra tilbyderne i de ulike landene. *Riksadvokaten* setter som en absolutt forutsetning for innføring av lagringsbestemmelser at det etableres systemer som sørger for at innsamlede data ikke kommer på avveie, men uttaler seg for øvrig ikke om lagringsstedet.

NorSIS, Norges Televisjon, NetCom, Telenor, Akademikerne, IKT-Norge, Politijuristene, HSH, ITAKT, Altibox, TDC, GET, Teknologirådet og *Forsvarergruppen av 1977* går alle inn for at tilbyderne selv skal velge lagringsløsning. De peker på den store sikkerhetsrisikoen som er knyttet til å samle alle data i en sentral database. Flere av disse peker også på at sentral lagring forsterker faren for andre personvernulemper, som formålsglidning, dobbeltlagring og uønsket kobling av data. *Post- og teletilsynet* går, av kostnadshensyn, også inn for at den enkelte tilbyder selv skal få velge lagringsløsning. Av sikkerhetshensyn går tilsynet primært inn for at data skal lagres i Norge.

IKT-Norge uttaler:

«IKT-Norge støtter høringsnotatets forslag om at det skal være valgfritt for selskapene om de ønsker å lagre data lokalt eller om de ønsker å gå sammen om en felles lagringsløsning. Det er imidlertid viktig at samlokalisert lagring må skje i regi av selskapene selv fremfor en myndighetskontrollert lagringsløsning. IKT-Norge støtter at selskaper som opererer i flere land må kunne samlokalisere. IKT-Norge mener at følgende krav fra høringsnotatet viser at dette direktivet ikke bidrar til harmonisering: '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'. Et slikt krav er etter IKT-Norges mening urimelig. IKT-Norge forutsetter videre at valg av lagringssted ikke vil ha implikasjoner for hvem som eventuelt skal bære kostnadene forbundet med lagringsplikten.»

Teknologirådet uttaler:

«Sentral lagring medfører sammenstilling av data fra ulike kilder. Den tyske forfatningsdomstolen besluttet i mars 2010 at den tyske implementeringen av datalagringsdirektivet er i strid med grunnloven. I sin begrunnelse går retten igjennom hvilke kriterier som må være til stede for at datalagring skal kunne aksepteres. En av faktorene som trekkes fram er nettopp viktigheten av at lagringen foretas av operatørene og ikke direkte av myndighetene. Dette betyr at dataene ikke er koblet sammen allerede gjennom lagringen (for eksempel ved ulike kundeforhold for mobiltelefoni, fasttelefoni og Internett), og medfører i mindre grad at lagringen kan oppleves som en totalkartlegging av alle borgernes kommunikasjonsaktiviteter».

NorSIS uttaler:

«NorSIS støtter at det ikke velges en sentral datalagringsløsning, slik at alle egg ikke havner i samme kurv. Når det er sagt, er noen av tilbyderne så store at deres datalagring vil innbefatte svært store datamengder, med persondata. NorSIS poengterer igjen viktigheten av å sette krav til sikring av data, tilgangskontroll og tilsyn av data slik at disse blir behandlet etter gjeldende lover og regler».

ICJ-Norge peker i sin høringsuttalelse på faren for lekkasjer og/eller tyveri av data, uavhengig av sikringskrav. De peker også på de betydelige utfordringene som er knyttet til at tilbyderne kan kjøpe lagringstjenester i andre EØS-land hvor norske myndigheter har liten eller ingen innvirkning på sikkerhets- og tilgangsreglene, og mener disse problemstillingene ikke er tilstrekkelig belyst i høringsnotatet.

Økokrim uttaler seg ikke direkte om valg av lagringssted, men gir på generelt grunnlag uttrykk for at forslaget i høringsnotatet, om at tilbyderne selv skal kunne velge lagringssted, med dagens teknologi vil kunne danne grunnlag for et sikkert system. Heller ikke *PST* kommenterer

valg av lagringssted spesielt, men synes i sine øvrige kommentarer å legge til grunn at data skal lagres lokalt hos tilbyder.

Datatilsynet har i sin høringsuttalelse uttalt at spørsmålet om implementering av direktivet først og fremst er et prinsipielt spørsmål og at det derfor er av underordnet betydning hvordan direktivet implementeres med tanke på lagringstid og lagringssted, men viser generelt til uttalelser fra de europeiske personvernmyndighetene (Artikkel 29-gruppen) hvor man har oppstilt konkrete krav til sikkerhetsforanstaltninger for datalagringen, og presiserer at disse må legges til grunn for en eventuell implementering. Artikkel 29-gruppens krav til sikkerhetsforanstaltninger forutsetter lokal lagring og krever at data lagret i henhold til datalagringsdirektivet skilles logisk fra data lagret for tilbydernes administrasjons- og faktureringsformål og at de omgis med tilstrekkelig sikkerhet, for eksempel ved at de krypteres.

11.4 Departementets vurdering

11.4.1 Informasjonssikkerhet

Departementet går inn for at det skal være opp til den enkelte tilbyder å velge lagringsløsning. Departementet har særlig vektlagt personvernmessige hensyn når det ikke foreslås å etablere en sentral lagringsløsning. Dette utelukker imidlertid ikke at små tilbydere kan gå sammen om en felles lagringsløsning. I tillegg til personvernmessige vurderinger har departementet også vurdert kostnader samt sikkerhetsmessige og konkurransemessige aspekter. Departementet mener informasjonssikkerheten kan ivaretas på en tilfredsstillende måte ved lokal lagring, og at sikkerheten ikke nødvendigvis blir bedre ivaretatt i en sentral database.

En sentral database vil innebære en samling av store mengder personopplysninger, noe som i seg selv kan utgjøre en stor personvernrisiko. Jo mer informasjon som er samlet på ett sted, jo større er skadepotensialet ved eventuelt misbruk eller uautorisert tilgang til dataene. En sentral base vil være mer sårbar for uautorisert tilgang og misbruk enn om dataene lagres lokalt. Samtidig vil en sentral base kunne gjøre det vanskeligere å forhindre formålsglidning over tid. Hvis store mengder personopplysninger skal samles på ett sted, bør det være særlig tungtveiende grunner for det, noe departementet ikke kan se er tilfellet her.

Datatilsynet har gitt uttrykk for at det kan oppstå tvil om behandlingsansvaret dersom data samles i en sentral database. Det vil være umulig for tilbyderne å beholde behandlingsansvaret med de plikter og det ansvar som ligger til denne funksjonen. Eventuelt må ansvaret tillegges en offentlig myndighet. Etter departementets vurdering er det heller ingen offentlig instans som utpeker seg som naturlig behandlingsansvarlig for en database som inneholder data om elektronisk kommunikasjon. Det er videre uklart i hvilken grad en tredjepart faktisk vil kunne oppfylle de forpliktelser som ligger til en behandlingsansvarlig, siden det vil gjelde opplysninger som denne parten har svært liten innflytelse over og kontroll med.

Departementet mener hensynet til trusselen om misbruk, det store skadepotensialet ved evt. sikkerhetsbrudd samt usikkerhet om behandlingsansvaret, er tungtveiende argumenter mot å etablere en sentral lagringsløsning.

Departementet ser at en sentral base vil kunne forenkle den praktiske prosessen for politiet med å få tilgang til data ved at de kan forholde seg til én virksomhet i stedet for et stort antall tilbydere. Departementet mener imidlertid det må være mulig å finne løsninger som forenkler den praktiske prosessen både for politiet og tilbyderne også ved en løsning med desentralisert lagring.

I henhold til datalagringsdirektivet er det ikke et krav at dataene skal lagres fysisk atskilt fra tilbyders øvrige data, men det skal etableres hensiktsmessige tekniske og organisatoriske anordninger for å ivareta datasikkerheten. Både Datatilsynet og ekomtilbyderne har gitt uttrykk for at de er enige i Artikkel 29-gruppens anbefaling om at det ved innføring av en eventuell lagringsplikt bør etableres et logisk skille mellom dataene avhengig av dataenes formål. Departementet vurderer det som avgjørende for å kunne kontrollere bruken av data som lagres i henhold til datalagringsdirektivet, at det stilles vilkår om et logisk skille mellom data til fakturerings- og administrasjonsformål på den ene siden, og data til kriminalitetsbekjempende formål på den andre siden. Dette innebærer ikke at data må lagres på to forskjellige steder, men at tilbyderne må ha mekanismer som styrer tilgangen til data avhengig av lagringsformål. Departementet går inn for at det innføres en plikt for tilbyderne til å sørge for lagringsløsninger som ivaretar sikkerheten rundt data lagret i henhold til datalagringsdirektivet. Departementet legger til grunn at etablering av tilstrekkelige sikkerhetsrutiner og -systemer er både teknisk og administrativt uproblematisk, men at det vil kreve en viss investering i lagringsløsninger for tilbyderne.

Departementet går inn for at data skal lagres på en måte som sikrer at data ikke er tilgjengelige

for andre enn relevant myndighet når rettens avgjørelse foreligger. Det må være et vilkår at data lagret for kriminalitetsbekjempende formål ikke skal være tilgjengelige for annet personell hos tilbyder enn de få som har tjenstlig behov.

Flere av høringsinstansene som har argumentert *for* sentral lagring, begrunner dette bl.a. med at det vil være enklere å sørge for tilstrekkelig sikkerhet. I henhold til datalagringsdirektivet, skal data som lagres for kriminalitetsbekjempelse være av samme kvalitet og nyte godt av samme beskyttelse og sikkerhetsforanstaltninger som øvrige data generert i det elektroniske kommunikasjonsnettet. Ansvaret for datasikkerhet og vern av personopplysninger om den enkelte bruker av elektronisk kommunikasjon, vil etter forslaget ligge hos den enkelte tilbyder, jf. personopplysningsloven § 13 og personopplysningsforskriften kapittel 2 og forslag til ny paragraf § 2-7 a i ekomloven.

Det er tilbyderne som med utgangspunkt i personopplysningsloven med forskrifter må foreta en trusselvurdering for å fastslå hvilke sikringstiltak som er nødvendige, og iverksette sikringstiltak i samsvar med konklusjonene fra en slik risikovurdering. En rekke ulike mekanismer for informasjonssikkerhet kan integreres i IKT-løsninger. Både sikringstiltak for å beskytte dataenes tilgjengelighet, konfidensialitet og integritet og kontroll og beskyttelse mot uautorisert eller ulovlig lagring, behandling, tilgjengeliggjøring og utlevering, kan være aktuelt å vurdere. Dette innebærer blant annet at det kan vurderes å fastsette bestemmelser som skal sikre at dataene er tilgjengelige når det er saklig behov for dem, at de ikke er tilgjengelige for andre enn de som har tjenstlig behov, at de ikke kan endres/manipuleres, samt at dataene er tilstrekkelig beskyttet mot utenforståendes tilgang. Departementet mener at informasjonssikkerheten i tilstrekkelig grad kan ivaretas ved en desentralisert lagringsløsning, også hos de tilbyderne som per i dag ikke har noe system for lagring.

Departementet har vurdert hvorvidt det bør innføres et krav om kryptering. De fleste høringsinstansene antyder at det bør stilles krav om kryptering ved sentral lagring, men temaet er i liten grad berørt når det gjelder lokal lagring. Departementet er i tvil om hvorvidt kryptering, etter en forholdsmessighetsvurdering, vil være et nødvendig sikringstiltak selv om det må betraktes som personvernfremmende. Departementet mener at spørsmålet om kryptering bør avgjøres av den enkelte tilbyder etter en konkret vurdering, og eventuelt etter nærmere kriterier som forutsettes fastsatt i forskrift.

I henhold til gjeldende rett, som foreslås videreført, er den enkelte tilbyder av elektroniske kommunikasjonstjenester ansvarlig for at data sikres på en betryggende måte. Tilbyderen skal gjennomføre planlagte og systematiske sikringstiltak jf. personopplysningsloven § 13. De sikringstiltak som er iverksatt, skal dokumenteres jf. personopplysningsloven § 14. Dokumentasjonen skal være tilgjengelig for Datatilsynet, og eventuelt også Personvernnemnda, på forespørsel. Dersom tilsynsmyndigheten vurderer de iverksatte sikringstiltakene som mangelfulle i forhold til den risiko behandlingen representerer, kan tilsynet fatte enkeltvedtak med pålegg om ytterligere sikring, herunder fastlegge kriterier for akseptabel risiko forbundet med behandlingen av personopplysninger, jf. personopplysningsforskriften § 2-2. Dette innebærer at dersom Datatilsynet vurderer at en tilbyder har foretatt mangelfull risikovurdering eller sikret data for dårlig, kan tilsynet fastlegge kriterier for akseptabel risiko som vil danne utgangspunkt for iverksetting av nødvendige sikringstiltak.

Behandling av personopplysninger i ekomsektoren for kundeadministrasjon, fakturering og gjennomføring av tjenester i forbindelse med abonnentens bruk av ekomnett, er konsesjonspliktig etter personopplysningsloven § 33 jf. personopplysningsforskriften § 2-1. Det vil være naturlig også å vurdere konsesjonsplikt for behandlinger som omfatter lagringspliktige data. På denne måten kan detaljert regulering av sikring av data pålegges gjennom vilkår i konsesjon som den enkelte tilbyder må innhente. Dette gir mulighet for å pålegge et bestemt sikkerhetsnivå som den enkelte tilbyder må forholde seg til.

I tillegg til at det foreslås en forskriftshjemmel i ekomloven § 2-7 a for regler om sikring av data, inneholder også personopplysningsloven § 13 en forskriftshjemmel for regler om sikring av personopplysninger. Det kan således fastsettes konkrete bestemmelser om sikring av lagringspliktige data både med hjemmel i ekomloven og med hjemmel i personopplysningsloven. Myndighetene har altså en rekke muligheter til å pålegge konkrete sikringstiltak, dersom det ved tilsyn eller i annen sammenheng skulle fremkomme at en tilbyder har for dårlig informasjonssikkerhet.

Departementet forutsetter at både Datatilsynet og Post- og teletilsynet vil føre et aktivt tilsyn med lagring av data i henhold til lagringsplikten for å sikre at tilbyderne holder et forsvarlig nivå på informasjonssikkerheten.

11.4.2 Lagringssted

Datalagringsdirektivet legger ingen føringer for hvordan lagrede data skal hentes ut eller overføres til myndigheten, men det fremgår av artikkel 8 at data skal lagres slik at de på anmodning fra kompetent myndighet kan overføres uten unødvendig forsinkelse.

I diskusjonen om lagringssted er det ikke tatt stilling til hvorvidt den fysiske lagringen må skje i Norge. Et krav om lagring på norsk territorium vil kunne anses som en begrensning av prinsippet om fri flyt av data innenfor EØS. Dette er en utfordring i forhold til datalagringsdirektivet, særlig med tanke på at det vil kunne gjelde ulike regler i ulike land både for lagringstid, informasjonssikkerhet og vilkår for uthenting av data. Departementet påpeker imidlertid at dersom det for eksempel er ulik lagringstid i det landet tilbyderen er etablert og i det landet tilbyderen ønsker å lagre sine data, er det førstnevnte lands regler som gjelder. Tilbydere som ønsker å lagre data i en felles konserndatabase i EU, må sørge for at data fra de ulike medlemslandene lagres på en måte som gjør at hvert enkelt medlemslands lover og regler når det gjelder lagringstid, vilkår for uthenting m.m. kan ivaretas. Direktivet forutsetter at medlemsstatene bistår hverandre i gjennomføringen av tilsyn på dette området. Dersom det på noe tidspunkt skulle bli aktuelt for en tilbyder å vurdere lagring av data i et land utenfor EØS-området, vil det avgjørende være om databehandleren kan tilby tilstrekkelig beskyttelse av personopplysningene. Overføring av personopplysninger til utlandet skal meldes til Datatilsynet som eventuelt kan sette vilkår for overføringen.

Departementet mener at muligheten for å føre tilsyn og kontroll med overholdelse av vilkårene for lagring og bruk er avgjørende, uavhengig av hvor lagringen skjer. Departementet viser her til EU-kommisjonens ekspertgruppe som har laget et utkast til veileder om nettopp denne problemstillingen. Her fremgår det at det er reglene i det landet der tilbyderen er etablert som skal gjelde.

12 Utlevering av data i etterforskningsøyemed

12.1 Gjeldende rett om politiets hjemler for innhenting av elektronisk lagrede data

Utgangspunktet er at *trafikk- og lokaliseringsdata* er taushetsbelagte opplysninger, jf. ekomloven § 2-9 første ledd. Utlevering av slike opplysninger krever derfor et særskilt hjemmelsgrunnlag. Politiet har i dag flere mulige hjemmelsgrunnlag for innhenting av historiske trafikkdata som til dels overlapper hverandre.

Fra denne taushetsplikten gjør ekomloven § 2-9 tredje ledd et unntak for abonnements- og brukerdata, det vil si visse opplysninger som knytter seg til identifikasjon, nærmere bestemt avtalebasert hemmelig telefonnummer og andre abonnementsopplysninger, samt elektronisk kommunikasjonsadresse. Høyesterett har avgjort at dette også omfatter dynamiske IP-adresser, jf. Rt. 1999 s. 1944. Av fjerde ledd følger det at anmodning fra politi eller påtalemyndighet om identifikasjonsdata skal etterkommes med mindre særlige forhold gjør det utilrådelig. I den videre fremstillingen knytter således utleveringsvilkårene seg til utlevering av trafikk- og lokaliseringsdata.

Beslag og utleveringspålegg – straffeprosessloven kapittel 16

Utlevering av historiske data kan skje etter reglene om beslag og utleveringspålegg. Det følger av straffeprosessloven §§ 203 og 210 at ting som kan ha betydning som bevis, enten kan beslaglegges av påtalemyndigheten eller retten kan pålegge besitteren å utlevere tingen. Elektronisk lagrede data er å regne som «ting» etter disse bestemmelsene. Dette ble slått fast av Høyesterett i Rt. 1992 side 904. Høyesterett uttalte her at begrensninger i lovens alminnelige adgang til beslag og krav om utlevering, utover det som er fastsatt i straffeprosessloven, krever særskilt hjemmel. 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. Antakelig må det samme gjelde for utleveringspålegg. 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. 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. § 118 første ledd 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 første ledd, 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 samme gjelder for utleveringspålegg. 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 for etterforskningen i saken», 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.

Etter straffeprosessloven § 215 a kan påtalemyndigheten som ledd i etterforskningen gi pålegg om sikring av elektronisk lagrede data. Dette gjelder både trafikkdata og innholdsdata, herunder filer med lyd, bilder eller tekst.

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. Dessuten må det antakelig også her innfortolkes et krav om skjellig grunn til mistanke om en bestemt straffbar handling.

Bestemmelsen gjelder data som 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.

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. 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.

Hensiktsmessighetsprinsippet og forholdsmessighetsprinsippet i straffeprosessloven § 170 a kommer til anvendelse ved bruk av disse tvangsmidlene. Det samme gjelder kommunikasjonskontroll etter straffeprosessloven kapittel 16 a som omtales nedenfor. Den som treffer beslutningen om å bruke et tvangsmiddel, 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. Det vises også til nærmere omtale av denne bestemmelsen ovenfor under kapittel 3.3.3.

Kommunikasjonskontroll – straffeprosessloven kapittel 16 a

Innhenting av historiske data skje med hjemmel i straffeprosessloven § 216 b om kommunikasjonskontroll. Annet ledd bokstav d gir hjemmel for å innhente data knyttet til kommunikasjon. Det gjelder opplysninger om hvilke kommunikasjonsanlegg som i et bestemt tidsrom skal settes eller har vært satt i forbindelse med et bestemt kommunikasjonsanlegg, og andre data knyttet til kommunikasjon. De opplysninger som omfattes er, for det første, opplysninger om hvilke kommunikasjonsanlegg som har kommunisert med et bestemt annet anlegg. Dette kan for eksempel være teleselskapenes registreringer av samtaler til og fra en telefon eller loggen over kommunikasjonen til og fra en datamaskin. Videre omfattes andre data knyttet til kommunikasjonen. Dette inkluderer blant annet opplysninger om samtalenes varighet, mobiltelefoners geografiske plassering idet samtalene finner sted (lokaliseringsopplysninger) og hvem som var logget inn på en datamaskin på det tidspunkt maskinen ble benyttet til kommunikasjon.

Pålegget må være knyttet til kommunikasjonsanlegg som mistenkte besitter eller kan antas å ville bruke eller ha brukt. Videre så må pålegget gjelde opplysninger om kommunikasjon som har funnet sted innenfor et bestemt tidsrom. Dette tidsrommet må angis i pålegget. For historiske data gjelder det ingen begrensning for hvilket tidsrom tillatelsen kan angi.

Vilkåret for utlevering av historiske data med hjemmel i bestemmelsen om kommunikasjonskontroll er at noen med skjellig grunn mistenkes for å ha begått en handling eller forsøk på handling som kan medføre fengsel i fem år eller mer. Slik tillatelse kan også gis der mistanken gjelder et narkotikalovbrudd, et narkotikarelatert heleri, sjikane, inngåelse av forbund om å begå en handling som kan straffes med fengsel i minst tre år og som skal begås som ledd i virksomheten til en organisert kriminell gruppe, befatning med barnepornografi, datainnbrudd eller enkelte forbrytelser mot rikets sikkerhet (straffeloven 1902 §§ 90, 91, 91 a, 94 jf. 90). Innhenting av historiske trafikkdata med hjemmel i straffeprosessloven § 216 b kan således skje i forbindelse med etterforskning av saker om lovbrudd av en viss grov-

het, samt i saker der en antar kommunikasjonskontroll vil være en særlig effektiv etterforskningsmetode. I tillegg 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 første ledd. Endelig vil straffeprosessloven § 170 a om hensiktsmessighetsprinsippet og forholdsmessighetsprinsippet komme til anvendelse også ved bruk av slike tvangsmidler, jf. ovenfor samt under kapittel 3.3.3.

Kommunikasjonskontroll etter § 216 b kan som utgangspunkt bare skje etter kjennelse fra retten. Straffeprosessloven § 216 d gir likevel påtalemyndigheten en hastekompetanse til å beslutte kommunikasjonskontroll. Slik beslutning må legges frem for retten innen 24 timer etter at kontrollen ble påbegynt.

Retten treffer beslutningen om kommunikasjonskontroll uten at den mistenkte eller den avgjørelsen rammer, gis adgang til å uttale seg, jf. straffeprosessloven § 216 e. 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 3. februar 1995 nr. 7 om kontroll med etterretnings-, overvåknings- og sikkerhetstjeneste. Kontrollutvalget er forutsatt særlig å skulle ivareta den enkeltes rettssikkerhet, jf. forskrift 31. mars 1995 nr. 281 om kommunikasjonskontroll § 14 første ledd.

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.

Andre hjemmelsgrunnlag

Dersom taushetsplikten oppheves med hjemmel i straffeprosessloven § 118 første ledd, er det formelt ikke noe til hinder for at tilbyder frivillig utleverer trafikkdata. Ifølge Post- og teletilsynet er imidlertid Telenor og NetCom, som er de to tilbyderne som politiet i praksis forholder seg til, blitt enige om å kreve beslutning om beslag for å utlevere trafikkdata.

Det har også 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. Den teknologiske utviklingen har trolig 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.

Teletilbyderne kan også utlevere opplysninger om en kundes teletrafikk dersom kunden samtykker til dette og dermed opphever taushetsplikten. Dette forutsetter imidlertid at kunden kan gis kjennskap til begjæringen.

Politiet vil også ha rett til tilgang til trafikkdata dersom vilkårene for nødrett er oppfylt.

12.2 Metodekontrollutvalgets forslag i NOU 2009: 15

Metodekontrollutvalget har i NOU 2009: 15 «Skjult informasjon – åpen kontroll» vurdert reglene for politiets innhenting av trafikkdata. De uttaler i utredningen kapittel 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 § 216 b. 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 tra-

fikkdata unntas fra teletilbyders taushetsplikt etter ekomloven § 2–9 dersom det foreligger beslutning om utleveringspålegg.»

Det fremgår av kapittel 20.5 på side 220 at utvalget også vurderte om straffeprosessloven § 216 b burde være den eneste hjemmelen for utlevering av historiske trafikkdata. Utvalget uttaler at dette ville ivareta hensynene til personvern og rettssikkerhet, men konkluderer likevel som følger:

«En slik endring vil imidlertid innebære en betydelig innstramming i politiets tilgang til trafikkdata i forhold til i dag. I dag kan politiet, i henhold til reglene om beslag og utleveringspålegg innhente trafikkdata knyttet til andre kommunikasjonsanlegg enn de mistenkte besitter eller antas å ville bruke, i saker med under fem års strafferamme og i saker der de øvrige vilkårene i kapittel 16 a ikke er oppfylt. Utvalget har kommet til at utlevering av trafikkdata til politiet ikke innebærer et så kraftig inngrep i de berørtes personvern at det er behov for en slik innstramming. Utvalget kan heller ikke se at dette vil svekke rettssikkerheten vesentlig.»

Utvalgets forslag innebærer at historiske trafikkdata fortsatt vil kunne innhentes både i form av utleveringspålegg og som del av kommunikasjonskontroll.

12.3 Datalagringsdirektivets betydning for reguleringen av tilgangen til lagrede data

Datalagringsdirektivet artikkel 4 lyder som følger (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.»

Bestemmelsen må forstås som en tilkjennegivelse av en forutsetning om nærmere nasjonal regulering og en henvisning til andre bestemmelser som kan begrense muligheten for å gi tilgang. I Generaladvokatens forslag til avgjørelse av saken som Irland anla om hjemmelsspørsmålet for direktivet (saksnr. 202/09), er artikkel 4 illustrerende nok beskrevet som en bestemmelse som «mere har karakter af en advarsel end en harmoniseringsforanstaltning» (punkt 104, dansk oversettelse).

Enkelte punkter i fortalen kaster likevel lys over denne bestemmelsen. Formålet med direktivet å bekjempe alvorlig kriminalitet, jf. direktivets fortale punkt 21 og artikkel 1 nr. 1, og det synes således som en forutsetning at data gjøres tilgjengelig for å oppklare alvorlige forbrytelser. Uttalelser om viktigheten av tilgang til data i arbeidet med å bekjempe organisert kriminalitet (punkt 7) og fordømmelsen av terrorisme (fortalen punkt 8 og 10) taler for at data bør gjøres tilgjengelig også for å bekjempe denne type kriminalitet.

Skranken for tilgangen til data ligger etter dette særlig i avveiningen mellom personvernhensyn og hensynet til kriminalitetsbekjempelse som kreves foretatt etter blant annet EMK artikkel 8 nr. 2 om inngrep i retten til privatliv, jf. kapittel 3. Ved denne vurderingen har statene en viss skjønnsmargin.

12.4 Høringsnotatets forslag

Lovendringsforslaget i høringsnotatet skiller mellom trafikkdata og lokaliseringsdata på den ene side, og abonnements- og brukerdata på den annen side.

Departementene foreslo å videreføre ordningen med at abonnements- og brukerdata kan utleveres til politi- og påtalemyndighet uavhengig av taushetsplikten.

Når det gjelder trafikkdata og lokaliseringsdata, la departementene til grunn at politi og påtalemyndighet måtte gis tilgang til disse, men at det ikke var nødvendig at også andre myndigheter ble gitt tilsvarende tilgang. Det ble vist til at 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. Det ble også vist til at det heller ikke i dag er adgang for andre myndigheter enn politiet til å bruke tvangsmidler etter straffeprosessloven som ledd i en straffesak.

Departementene la også til grunn at det er behov for en skjerping av vilkårene for tilgang til

trafikkdata og lokaliseringsdata for å imøtekomme direktivets krav om særlige grunner og dets formål om å bekjempe grov kriminalitet. Endringen ble foreslått gjennomført i form av et nytt annet punktum i straffeprosessloven § 210 første ledd om utleveringspålegg som skjerper vilkårene for utlevering av data sammenlignet med vilkårene som ellers gjelder for utleveringspålegg. Etter forslaget skulle utlevering av lagringspliktige data etter ekomloven § 2-8 annet ledd bare kunne pålegges dersom det straffbare forholdet har en strafferamme på fengsel i 3 år eller mer. Treårsgrensen ble blant annet begrunnet med at den ville innebære en betydelig skjerpelse i forhold til gjeldende generelle vilkår for utleveringspålegg. Samtidig ble det antatt at den burde settes lavere enn i straffeprosessloven § 216 b om bl.a. kommunikasjonskontroll i sanntid og fremtid, ettersom dette regnes som ekstraordinære etterforskningsmidler.

Departementene la videre til grunn at visse forbrytelser som har en lavere strafferamme enn tre år kunne være særlig vanskelige å etterforske uten bruk av data og at også slike saker kunne vurderes som «særlige saker». Som eksempler på slike saker ble nevnt spionasje, terrorvirksomhet, brudd på taushetsplikt ilagt av retten i forbindelse med benyttede tvangsmidler som ransaking eller beslag, datainnbrudd, telefonavlytting, narkotikalovbrudd, hvitvasking, forstyrrelse av privatlivets fred, og enkelte seksuallovbrudd mot barn. De aktuelle paragrafene i straffeloven 1902 ble foreslått særskilt oppregnet i forslaget til endring av straffeprosessloven § 210 første ledd som alternativer til det generelle treårs strafferammekravet. Departementene ba spesielt om høringsinstansenes syn på denne oppregningen.

Av rettssikkerhetshensyn ble det foreslått at påtalemyndigheten heretter bare skulle kunne få tilgang til data etter rettens kjennelse. Rettens vurdering ble antatt i all hovedsak å være sammenfellende med den vurderingen Post- og teletilsynet foretar når det vurderer spørsmålet om fritak fra taushetsplikten, jf. straffeprosessloven §§ 204 og 210 jf. § 118. Det ble derfor samtidig foreslått å løse Post- og teletilsynet fra denne oppgaven.

Det ble i høringsnotatet ikke foreslått endringer i gjeldende § 210 annet ledd som gir påtalemyndigheten en hastekompetanse til å beslutte utleveringspålegg dersom det ved opphold er fare for at etterforskningen vil lide.

Det ble også foreslått en ytterligere innskjerping i forhold til gjeldende rett ved innføringen av kravet om at politiet må godtgjøre at «noen med skjellig grunn mistenkes». Departementet vurderte som et alternativ å lovfeste kravet til skjellig grunn, men uten krav om at mistanken må knytte seg til en konkret person. Dette ble forkastet med følgende begrunnelse:

> «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 ba på denne bakgrunn spesielt om høringsinstansenes syn på utformingen av dette vilkåret.

12.5 Høringsinstansenes syn

12.5.1 Vilkårene for utlevering av data

Flere av høringsinstansene innenfor politi- og påtalemyndighet er kritiske til at det foreslås en innstramming av vilkårene for utlevering av trafikkdata. *Politidirektoratet* viser til at trafikkdata har vært innhentet i lang tid, til at det ikke har vært reist kritikk mot denne praksisen, og til Metodekontrollutvalgets beskrivelse av slik innhenting som relativt lite inngripende, og spør om det er nødvendig å skjerpe vilkårene. *Kripos* uttaler:

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

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

I uttalelsen redegjøres det så for endringen av straffeprosessloven § 210 tredje ledd ved lov 25. juni 2004 nr. 52, hvoretter påtalemyndigheten ble gitt kompetanse til å pålegge utlevering av dokumenter mv. fra banker og finansinstitusjoner, og vurderingene som ble foretatt i forarbeidene til lovendringen. Kripos oppsummerer deretter slik:

«Ved en implementering av datalagringsdirektivet i norsk rett kan en ikke se bort fra disse vurderingene. Dette særlig fordi trafikkdata er et bevis det allerede har vært mulig å benytte i etterforskningsøyemed her i landet siden 90-tallet, og hvor vilkår og kompetanse for innhenting for lengst er innarbeidet i eksisterende straffeprosessuelle hjemler. På denne bakgrunn foreslås prinsipalt at det ikke foretas noen endringer i nåværende § 210 første ledd, men at trafikkdata omfattes som før.»

Oslo statsadvokatembeter er også kritisk til det de beskriver som en betydelig innstramming av dagens regler for utlevering av trafikkdata og foreslår isteden en gradering av vilkårene avhengig av den tid som er gått siden forbrytelsen fant sted. Embetet argumenterer med at man på den måten kunne beholde dagens regler for data som ikke er eldre enn seks måneder, samtidig som man innførte skjerpede regler for data lagret i mer enn seks måneder.

Post- og teletilsynet stiller spørsmål ved om det bør differensieres mellom vilkår for tilgang til trafikkdata og lokaliseringsdata:

«Man kan f. eks tenke seg særskilte vilkår for utlevering av data for basestasjonssøk (der personvernet til flere personer kan bli krenket) om at handlingen må omfattes av en bestemmelse som gir en høyere strafferamme enn ved utlevering av trafikkdata knyttet til en enkeltperson. I forlengelse av dette foreslår PT at straffeprosessloven § 216 c annet ledd om særlige grunner gis tilsvarende anvendelse ved utlevering av trafikkdata etter den foreslåtte bestemmelse i straffeprosessloven § 210. Dette for at personvernet skal kunne ivaretas på best mulig måte.»

Telenor ser at forslaget om skjerpede vilkår for tilgang til trafikkdata kan være for snever for politiet og nevner muligheten for differensiert tilgang avhengig av formålet med lagringen som et mulig alternativ:

«Det er i prinsippet ikke opp til Telenor å vurdere denne siden av saken, men man kan kanskje se for seg en viss adgang til utlevering av data tilbyderne sitter med, uavhengig av lagringsplikten, uten at de skjerpede krav får anvendelse. Det vil i så fall kreve en form for separasjon av de forskjellige typer data hos tilbyderne, basert på om de er lagret i henhold til lagringsplikten eller om de er lagret av hensyn til tilbyderens eget bruk (fakturering, gjennomføring av tjenester og lignende). Dette vil igjen kunne by på utfordringer i tilbydernes datasystemer, både av praktisk og kostnadsmessig karakter.»

12.5.2 Kravet om mistanke til en bestemt person

Samtlige instanser innenfor politi- og påtalemyndighet går sterkt imot forslaget om å innføre et slikt krav. *Politidirektoratet* skriver følgende:

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

Riksadvokaten påpeker også at et krav om at mistanken må kunne knyttes til en bestemt person vil avskjære muligheten for å innhente trafikkdata i en rekke saker, og at slik innhenting ofte nettopp har som formål å identifisere en antatt gjerningsperson. Embetet uttaler samtidig at man ikke har motforestillinger til at kravet om skjellig grunn til mistanke om en bestemt straffbar handling lov-

festes samtidig som det innføres som vilkår for tilgang at trafikkdata må være av vesentlig betydning for etterforskningen. *Oslo statsadvokatembeter, Politiets sikkerhetstjeneste (PST), Økokrim, Politiets Fellesforbund* og *Politijuristene* har uttalelser som går i samme retning.

Kripos begrunner sin motstand mot det foreslåtte kravet om skjellig grunn til mistanke mot en bestemt person slik:

> «De senere årene har det vært flere tilfeller av trusler mot skoler. I en innledende fase av etterforskningen kan mistanken rette seg mot flere personer, uten at det foreligger skjellig grunn til mistanke mot noen av disse. Dersom forslaget vedtas vil det redusere muligheten til å identifisere gjerningspersoner i disse sakene. Siden dette ofte er mindreårige som trenger samfunnets hjelp, og som utgjør en potensielt stor trussel mot både eget og andres liv, er det uheldig dersom politiet mister muligheten til å benytte trafikkdata til å fange dem opp.
>
> Videre er det relevant å sammenligne forslaget til ny § 210 med vilkårene for utvidet ransaking, jf. straffeprosessloven kapittel 15. § 192 tredje ledd hjemler såkalt 3. mannsransaking, hvoretter det må foreligge skjellig grunn til mistanke om en straffbar handling. Det er imidlertid ikke krav om at mistanken er rettet mot en bestemt person. Videre kan politiet i etterforskningsøyemed, med hjemmel i § 193, foreta ransaking av alle steder som etter sin art er tilgjengelig for alle. På samme måte kan politiet ransake militære bygninger og rom. At vilkårene for å innhente trafikkdata skal være andre – og presumptivt strengere – enn vilkårene for å ransake – gir en ubalanse i lovverket.
>
> Forslaget rammer også politiets mulighet til å etterforske andre forhold enn de som umiddelbart framstår som straffbare. Straffeprosessloven § 224 fastslår at 'etterforskning foretas når det som følge av anmeldelse eller andre omstendigheter er rimelig grunn til å undersøke om det foreligger straffbart forhold som forfølges av det offentlige', og med hjemmel i siste ledd 'kan' det ved brann og andre ulykker foretas etterforskning om årsaken 'selv om det ikke er grunn til mistanke om et straffbart forhold'. Å etterforske slike saker utgjør en vesentlig del av politiets oppgaver, og trafikkdata brukes regelmessig i etterforskningen. […]
>
> De eksisterende straffeprosessuelle hjemler dekker de aller fleste tilfeller hvor det er aktuelt å innhente trafikkdata. I tilfeller hvor nødrett påberopes som grunnlag er dette normalt på grunn av tidsaspektet, og ikke fordi vilkårene for å innhente trafikkdata ikke er til stede. Dersom datalagringsdirektivet innføres på de foreslåtte vilkår vil det stille seg annerledes.
>
> Saknetsakene er et godt eksempel på dette. Når pårørende melder en person saknet, har politiet en plikt til å undersøke forholdet. Innhenting av trafikkdata vil være et relevant etterforskningsskritt. I et slikt tilfelle kan riktignok nødrettsbestemmelsen i strl § 47 anvendes, men det er neppe noen god løsning fra lovgivers side å overlate alle slike vurderinger til utøvende myndigheter. Inngrepets art tilsier en klar lovhjemmel, blant annet av hensyn til forutberegneligheten. Nødrettsbestemmelsen er ment å være en snever sikkerhetsventil som kun kommer til anvendelse dersom handlingen ikke har (annen) hjemmel i lov.
>
> På denne bakgrunn anbefaler Kripos at det ikke oppstilles noe vilkår om at det må foreligge skjellig grunn til mistanke mot en bestemt person. Subsidiært må det i så fall lovfestes et unntak for etterforskning hjemlet i strpl § 224 fjerde ledd, samt saknetsaker og redningsaksjoner.
>
> Videre må bestemmelsen formuleres slik at også stedsspesifikke spor kan innhentes uavhengig av om noen bestemt person kan mistenkes for handlingen.»

Økokrim uttaler:

> «Departementenes høringsforslag bygger på en anerkjennelse av at enkelte typer lovbrudd er 'særskilt vanskelig å etterforske uten tilgang til data'. I relasjon til disse fremstår kravet om at skjellig grunn til mistanke må foreligge før man får tilgang til data paradoksalt, ettersom det ligger i erkjennelsen av disse vanskelighetene at det også vil være vanskelig å etablere skjellig grunn til mistanke uten tilgang til data. Opprettholdes kravet om skjellig grunn i slike saker, er det sannsynlig at mange lovbrytere hvis skyld kunne vært påvist ved tilgang til trafikkdata, vil gå fri fordi det uten slike data ikke en gang kan påvises skjellig grunn til mistanke.
>
> Dette vil for eksempel gjelde etterforskingen av handlinger der kommunikasjonen er den eneste komponenten som skiller en straffbar handling fra en lovlig handling, altså der det er selve kommunikasjonen som gjør handlingen ulovlig, jf. også ovenfor i punkt 1.3 om betydningen av trafikkdata for etterforskingen

av slike handlinger. I slike tilfelle vil trafikkdata være essensielle for i det hele tatt å påvise skjellig grunn til mistanke. For ØKOKRIMs del gjelder dette særlig i etterforskingen av verdipapirkriminalitet, der det ulovlige består i kommunikasjon mellom parter.»

Også *Stine Sofies Stiftelse* er mot innføring av et krav om skjellig grunn til mistanke mot en bestemt person. Stiftelsen spør hvordan dette vil fungere i forhold til for eksempel en pedofiliring, hvor det kan være mistanke mot en bestemt krets av personer, og fremholder at i slike saker må hensynet til barns rettssikkerhet veie tyngst.

Institutt for rettsinformatikk ved Universitetet i Oslo og *NITO* er positive til forslaget er at politiet må godtgjøre at noen med skjellig grunn kan mistenkes før data kan utleveres. Det samme er *Post- og teletilsynet* som har følgende merknader:

«PTs praksis i dag er at den som rammes av en fritaksbegjæring må ha straffeprosessuell stilling som enten mistenkt eller siktet. Forslaget innebærer derfor en heving av minstekravet til hvor sterk mistanken må være for at trafikkdata kan utleveres. Verdien av trafikkdata for politiet i etterforskingen antas dermed å bli noe redusert. Sett i lys av den forlengede lagringstiden, finner imidlertid PT å kunne støtte dette.

Slik PT forstår departementenes forslag, er det eneste kravet til tilknytning mellom mistenkte og det abonnement det begjæres utlevert trafikkdata på, er at trafikkdataene som begjæres utlevert 'antas å ha betydning som bevis'. I praksis innebærer dette at hvis person A med skjellig grunn mistenkes for en handling som rammes av en straffbar handling som kan straffes med fengsel i tre år eller mer, så kan politiet begjære utlevert all trafikkdata som antas å ha betydning som bevis, uavhengig av hvem som har generert den. Etter PTs praksis i dag samtykkes kun til utlevering av trafikkdata på abonnement som har vært disponert av mistenkte/siktede. På dette punkt vil forslaget kunne medføre utlevering av trafikkdata utelukkende generert av andre enn siktede. Etter PTs syn er dette ikke heldig og bør unngås. For kommunikasjonskontroll er dette tilknytningskravet løst i straffeprosessloven § 216a tredje ledd. Det foreslås at denne bestemmelse gis tilsvarende anvendelse for utlevering av trafikkdata etter straffeprosessloven § 210 første ledd nytt annet punktum.

I PTs praksis er det et unntak fra kravet om at mistenkte/siktede må ha disponert det abonnement som det kreves utlevert trafikkdata på. Det er i de tilfeller hvor vedkommende trafikkdataene relaterer seg til ikke kan eller ikke kan forventes å kunne gi et kvalifisert samtykke til utlevering av trafikkdata. Det typiske eksemplet er i tilfeller utlevering av trafikkdata på telefoner disponert av avdøde i en drapssak. Andre tilfeller er vitner/fornærmede i såkalte 'trafficingsaker', som trolig ikke vil kunne gi et kvalifisert samtykke til utlevering av trafikkdata. I slike saker tilsier PTs praksis at det kan gis samtykke til utlevering. Dette bør opprettholdes, og behandles innenfor samme tilgangsregime.

PT forstår departementenes forslag slik at det er en identifisert person som med 'skjellig grunn' må mistenkes for at inngangskriteriene skal anses oppfylt. De tilfeller hvor politiet med skjellig grunn mistenker at det er begått en handling som kan straffes med fengsel i tre år eller mer, men hvor mistanken ikke er rettet mot noen identifisert person kan altså ikke foranledige utlevering av trafikkdata. Typiske saker hvor denne muligheten benyttes er drap, ran, voldtekt, innbrudd, ildspåsettelse eller andre saker hvor åsted og tid for den kriminelle handling er kjent. I slike tilfelle er det etter dagens praksis mulig å gjennomføre basestasjonssøk for det aktuelle åstedet. I den grad PTs forståelse er korrekt og dette ikke er tilsiktet bør det inntas et tillegg for slike situasjoner.»

12.5.3 Kravet om tre års strafferamme

De fleste av høringsinstansene innenfor politi- og påtalemyndighet er kritiske til forslaget om å innføre strafferammekrav for politiets tilgang til trafikkdata.

Politidirektoratet viser til at dagens bestemmelser om beslag ikke krever at den straffbare handlingen er av en viss grovhet. Med henvisning til Follo politidistrikts uttalelse uttaler direktoratet at det kan

«virke inkonsekvent med et så strengt inngangsvilkår når en ellers i straffeprosessen for eksempel opererer med 'fengsel i 6 måneder' for pågripelse og varetektsfengsling (strpl § 171), eller 'frihetsstraff' for ransaking av person, bopel m.v. (strpl § 192).»

Politidirektoratet slutter seg til *Søndre Buskerud politidistrikts* syn om at begrensningen må ligge i en betraktning om at trafikkdata er nødvendig sett

i forhold til den etterforskning som skal utføres og vurdert ut fra en forholdsmessighetsvurdering, jf. strpl. § 170 a. Økokrim uttaler seg i samme retning.

Søndre Buskerud politidistrikt påpeker også at det lett vil kunne tenkes handlinger som i realiteten fremstår som alvorlige selv om strafferammen er under tre år, for eksempel gjentatte straffbare handlinger hvor strafferammen er lav, men som samlet sett fremstår som mer alvorlig. *Follo politidistrikt* nevner at blant annet legemsfornærmelse med skadefølge faller utenfor, og mener dette kan slå uheldig ut i forhold til etterforskningen av voldssaker som for øvrig er særlig prioriterte.

Politiets fellesforbund mener innskjerpingen vil kunne begrense politiets muligheter til å oppklare alvorlig kriminalitet og begrunner dette med følgende eksempler:

> «Som eksempel på viktige saker hvor det kan bli vanskelig å få tilgang til trafikkdata dersom foreslåtte strafferamme innføres, er saker der barn og unge blir utsatt for mobbing, trakassering, «grooming», sjikane eller trusler via Internett/mobiltelefon. Dette er intet ukjent fenomen i dagens samfunn, og et særdeles viktig område å sette inn ressurser på.
>
> Et annet område som kan nevnes er miljøkriminalitet. Lave strafferammer vil gjøre at sakene blir desto vanskeligere å etterforske dersom man i fremtiden ikke får tilgang til viktig trafikkdata.
>
> I tillegg ønsker vi å trekke frem en sak fra Rogaland som på en god måte kan eksemplifisere at store sakskompleks ofte begynner i det små. Det kan i initialfasen av en etterforskning være vanskelig å se omfanget av sakskomplekset. Noe som i startfasen kan fremstå som et simpelt tyveri, kan vise seg å være organisert kriminalitet.
>
> *Tyverier av minibankkort på restauranter med påfølgende uttak i minibank.*
> Tidlig i juli 2009 ble en rumensk statsborger pågrepet etter tips fra et av utestedene. Han var i besittelse av et stjålet minibankkort som ble knyttet til en av utestedets kunder. Siktede var i besittelse av en mobiltelefon og anropsloggen viste fersk kontakt med to andre mobiltelefoner. Trafikkdata ble innhentet etter samtykke fra Post- & Teletilsynet.
>
> En analyse av innhentet trafikkdata viste at alle tre telefonnumrene i perioden trafikkdata var tilgjengelig, hadde hatt samme 'reiserute' mellom Stavanger og Bergen og at personene som disponerte telefonnumrene hadde mye kontakt med hverandre. Det ble opprettet samarbeid med politiet i Haugesund og Bergen for en koordinering av etterforskningen av tilsvarende saker. Trafikkdata var med på å identifisere de to andre personene. Dette medførte at to personer ble pågrepet i Troms politidistrikt.
>
> Trafikkdata på alle tre gjerningsmennene knyttet de til geografisk områder over en periode på ca 3 mnd. Dette ble sammenholdt med gjerningssted og gjerningstidspunkt. Etterforskningen endte med tiltale på 122 forhold for tyveri fra person på offentlig sted i Berge, haugesund og Stavanger.
>
> Uten trafikkdata hadde det vært vanskelig å bevise noe annet enn det ene tyveriet førstemann ble pågrepet for.
>
> For øvrig har politiet via andre kanaler identifisert at alle tre personer har vært i Norge i lenger tid enn 3 mnd. Hvis lagring av trafikkdata har vært lenger enn 3 mnd ville politiet trolig hatt mulighet til å oppklare forhold rumenerne kunne mistenkes for, forut for den perioden trafikkdata var tilgjengelig.

PF mener at intensjonen med direktivet kan bli undergravet om en innfører en strafferamme på fengsel i tre år eller mer, jf. ovennevnte eksempler. Vi mener videre at ved en eventuell innføring av krav om oppgitt strafferamme, må det nedsettes en arbeidsgruppe som bør se på aktuelle unntak fra bestemmelsen. Unntakene bør omfatte viktig lovbrudd som ikke innehar en strafferamme på 3 år eller mer, og som dermed vil kunne ivareta rettssikkerheten.»

Kripos er kritisk til kravet om tre års stafferamme. De peker på at dette synes inkonsekvent i forhold til straffeprosessloven § 215 a om sikringspålegg:

> «Strpl § 215 a, hvoretter påtalemyndigheten kan gi sikringspålegg, har samme inngangsvilkår som §§ 203 og 210, nemlig at dataene «antas å ha betydning som bevis» i etterforskningen. I Ot.prp.nr. 40 (2004-2005) fastslås at bestemmelsen omfatter trafikkdata. Dersom § 210 endres som foreslått i høringsnotatet, uten at det samtidig gjøres en endring i § 215a, vil det medføre at påtalemyndigheten har en langt videre adgang til å gi sikringspålegg enn

det domstolene vil ha til å pålegge utlevering av de samme dataene. Dette illustrerer at vilkårene som foreslås i høringsnotatet vil gi et inkonsekvent nasjonalt regelverk.

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

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

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

Oslo statsadvokatembeter uttaler derimot at de ikke har vesentlige innvendinger mot det foreslåtte strafferammekravet og de særskilt oppregnede straffebudene som strafferammekravet ikke gjelder for. *Telemark politidistrikt* mener treårskravet er godt begrunnet og vil innebære at utlevering vil kunne skje ved etterforskning av de mer alvorlige forholdene.

Flere av de øvrige høringsinstansene stiller spørsmål ved om den foreslåtte strafferammen gir en tilstrekkelig avgrensning av politiets mulighet for tilgang til data. Blant disse er *Post- og teletilsynet* som viser til at strafferammen for eksempelvis simpelt tyveri er inntil tre år og at forslaget dermed innebærer at politiet også kan innhente trafikkdata i slike typer saker. *Advokatforeningen* uttaler:

«I debatten trekkes gjerne frem behovet for å hindre organisert kriminalitet og terrorisme, men forslaget innebærer at lagret informasjon kan brukes i etterforskningen av all kriminalitet med strafferamme på 3 år eller mer og i noen tilfeller også mindre alvorlig kriminalitet. Dette innebærer for så vidt en betydelig innskjerping i forhold til dagens krav om utlevering av ting som kan ha betydning som bevis i en straffesak, jf. strpl § 210, hvoretter retten kan pålegge den som besitter slikt materiale å utlevere dette. Men kravene er mindre strenge enn dagens regler om kontroll av kommunikasjonsanlegg, jf. strpl § 216 b. I høringsnotatet (på s. 47) er dette begrunnet med at lagring og bruk etter de nye reglene i datalagringsdirektivet er et mindre inngripende tvangsmiddel og at det således er naturlig at terskelen er lavere. Forslaget går altså lengre enn å bekjempe terrorisme og organisert kriminalitet. De nye reglene innfører et verktøy som vil kunne brukes i betydelig omfang i politiets etterforskning av ordinær kriminalitet.»

Forsvarergruppen av 1977 synes langt på vei å dele Advokatforeningens syn. De mener for øvrig at strafferammekravet ikke bør gjelde der innhenting skjer for å forebygge at noen uskyldig blir straffet, og viser til parallellen i taushetspliktbestemmelsen om sterk taushetsplikt i straffeprosessloven § 119 tredje ledd.

IKT-Norge mener man i høringsnotatet har lagt seg på en for liberal tolkning av begrepet «serious crime». Organisasjonen vil heve strafferammekravet og begrunner dette blant annet som følger:

«Direktivets formål var bekjempelse av terror og alvorlig organisert kriminalitet. Dette bør også være normgivende for den norske implementeringen. Vi mener derfor at kravet om at data skal utleveres dersom det straffbare forholdet har en strafferamme på 3 år eller mer er urimelig lavt. Vi ønsker i den forbindelse også å vise til våre nordiske naboland Finland og Danmark som har lagt seg på henholdsvis 4 år

og 6 år. IKT-Norge har ingen konkrete forslag til hvilken strafferamme man bør legge seg på eller til den oppregning av lovbrudd som er foreslått som alternativ til det generelle kravet. Dersom direktivet skal implementeres i Norge mener IKT-Norge at man ikke skal gå ut over direktivets minstekrav. Det betyr at vi anbefaler at Norge legger seg på en restriktiv linje og setter listen høyt for når politiets skal få tilgang til data. Dette skyldes blant annet at vi frykter en «slippery slope» utvikling der listen legges lavere og lavere. Det virker opplagt at forslaget i høringsnotatet er betydelig annerledes enn direktivets opprinnelige tekst.»

Forbrukerrådet viser til Danmark, hvor grensen er satt ved en strafferamme på 6 år, og mener høringsnotatet redegjør dårlig for hvorfor man ikke kan ha samme grense i norsk rett. Lovbrudd som det er særlig vanskelig å etterforske uten tilgang til data plasseres i samme kategori som grov kriminalitet.

NorSIS mener at de nordiske land bør tilstrebe samme strafferammekrav for uthenting av data, og viser til at Sverige og Finland har strengere krav enn det norske forslaget.

12.5.4 Domstolskontroll med utlevering av data

Møre og Romsdal og Sogn og Fjordane statsadvokatembeter, *Akademikerne, NITO* og *Forsvarergruppen av 1977* støtter forslaget om at bare retten skal kunne pålegge besitteren å utlevere data. Også *PST* oppfattes å støtte dette forslaget. *Forsvarergruppen* uttaler:

«Den personvernmessige sensitivitet av dataene tilsier uten videre at dette bør undergis strengere regler enn beslag og utleveringspålegg ellers. Dette gjelder særlig idet opplysninger som først er innhentet i en straffesak senest på tidspunktet for uttak av tiltale blir tilgjengelig for samtlige aktører, herunder siktede og fornærmede. Opplysningene er således i praksis ikke beskyttet av taushetsplikt etter at innhenting er besluttet.»

NITO mener i tillegg at forslaget bør suppleres med en ordning med at en ombudsmann taler enkeltindividets sak i retten.

Post- og teletilsynet ønsker ikke å komme med noen klar anbefaling om hvem som skal ha avgjørelsesmyndigheten, men peker på at domstolenes erfaring med de foreslåtte vurderingstema, bevisvurdering og forholdsmessighetsvurdering taler for av avgjørelsesmyndigheten legges hit. Tilsynet mener samtidig at behovet for å sikre nasjonal likebehandling kan tale mot desentralisert domstolsbehandling. Videre heter det i høringsuttalelsen herfra:

«Tradisjonelt har maktfordelingsprinsippet medført at avgjørelsesmyndigheten i slike saker legges til domstolene. Legges avgjørelsesmyndigheten til PT vil imidlertid det parlamentariske ansvar og Stortingets kontroll med forvaltningen medføre at Stortinget vil kunne kontrollere praksisen. Avhengig av hvilken klagebehandlingsmåte som velges, vil det også kunne etableres forvaltningsmessig kontroll. Å legge avgjørelsesmyndigheten til forvaltningen muliggjør også opprettelsen av særskilte kontrollutvalg som ikke vil bli påført de åpenbare begrensninger kontrollutvalg som skal kontrollere domstolens praksis påføres.»

Flere høringsinstanser innenfor politi- og påtalemyndighet er kritiske til forslaget om at krav om utlevering av trafikkdata skal behandles av retten. *Politiets fellesforbund* frykter at forslaget vil forsinke etterforskningen av straffesaker betraktelig. *Riksadvokaten, Kripos, Oslo politidistrikt* og *Politidirektoratet* peker på at et krav om utleveringspålegg fra retten for innhenting av denne typen bevis vil bryte med dagens system og stiller spørsmål ved behovet for overføring av kompetanse fra påtalemyndigheten til domstolene. *Oslo politidistrikt*, med tilslutning fra *Politidirektoratet*, utdyper sitt syn slik:

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

En overføring av myndigheten til retten, vil bidra til en vesentlig økt saksbehandling og ressursbruk hos politiet, påtalemyndigheten og tingretten. I hver enkelt sak må tingretten få oversendt påtegning med begrunnelse for begjæringen og kopi av samtlige saksdokumenter – pr. i dag er dette omlag 1900 saker

> årlig. Dette vil være en unødvendig tapping av politiets og tingrettens ressurser, uten at det vil være et begrunnet bidrag til økt rettssikkerhet.»

Kripos peker samtidig på at en ordning med domstolsprøving har den fordel at den bidrar til å sikre ensartet praksis. *Kripos* uttaler videre:

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

Flere høringsinstanser innenfor politi- og påtalemyndighet understreker behovet for hastekompetanse for påtalemyndigheten, alternativt vaktordning ved domstolene.

Tele 2 er ikke overbevist om at alle landets tingretter er mer kompetent enn Post- og teletilsynet på dette området og antar at tilsynet fortsatt bør ha en rolle.

HSH støtter forslaget om å løse Post- og teletilsynet fra oppgaven med å frita tilbyder fra taushetsplikten og la retten avgjøre om dataene skal utleveres. *IKT-Norge* mener derimot at Post- og teletilsynet, som skal ivareta Ekomlovens formål og virke, fortsatt bør ha en rolle i sakene om politiets tilgang til data for etterforskning og forebygging av alvorlig kriminalitet. Det samme mener *Telenor*. Selskapet støtter intensjonen bak forslaget om domstolsbehandling, men uttaler samtidig:

> «Hvis domstolsbehandling skal representere en reell terskelhevning i forhold til dagens utleveringsregler, kreves det imidlertid at domstolene i praksis foretar en vurdering av alle sider ved utleveringen, ikke minst det straffeprosessuelle kravet om forholdsmessighet mellom hensynet til kriminalitetsbekjempelse og hensynet til personvernet, jf. straffeprosessloven § 170 a, som også er berørt i departementets notat. Det er Telenors oppfatning at denne vurderingen – etter dagens ordning – har vært foretatt på en meget samvittighets- og innsiktsfull måte av PT i forbindelse med tilsynets vurdering av om den lovbestemte taushetsplikt i den enkelte sak kan fravikes.»

Etter deres syn gjør Post- og teletilsynets kompetanse om ekombransjen og elektroniske spor, at tilsynet ofte vil være bedre i stand til å vurdere relevansen og konsekvensen av politiets krav om utlevering av data enn domstolene. Telenor er bekymret for konsekvensen dersom tilsynet fratas oppgaven med å vurdere spørsmål om fritak fra taushetsplikten for de lagrede dataene før retten fatter sin beslutning, og spør om ikke PT fortsatt bør ha ansvaret for å vurdere politiets begjæring om utlevering av data opp mot den lovbestemte taushetsplikten og det straffeprosessuelle forholdsmessighetsprinsipp, slik straffeprosessloven § 118 første ledd forutsetter. Domstolen vil uansett ha en mulighet til å overprøve PTs vurdering etter § 118 annet ledd. Telenor forutsetter for øvrig at de skjerpede kravene for utlevering, herunder domstolsbehandling, ikke gjelder informasjon som er omfattet av ekomloven § 2-9 tredje ledd, slik at politiet fortsatt kan få direkte tilgang til abonnentinformasjon fra tilbyderne, uten å gå veien om domstolene.

12.6 Departementets vurdering

Abonnementsopplysninger, herunder også elektronisk kommunikasjonsadresse, er gjennomgående å anse som mindre beskyttelsesverdige opplysninger enn trafikkdata og lokaliseringsdata. Å oppgi for eksempel hemmelig telefonnummer og IP-adresse utgjør vanligvis et mer beskjedent innhugg i personvernet enn utlevering av trafikkdata og lokaliseringsdata. Etter departementets syn kan det derfor forsvares å gi større tilgang til abonnementsopplysninger enn trafikkdata. Det foreslås således ingen endringer i gjeldende rett (ekomloven § 2-9 tredje ledd) for så vidt gjelder slike opplysninger.

Hovedregelen om utlevering av historiske, personspesifikke trafikkdata foreslås nedfelt i straffeprosessloven § 210 b. Strafferammekravet foreslås utformet slik at alle straffebestemmelser som kan medføre straff av fengsel i 4 år eller mer, kan begrunne utlevering av data.

Dette forslaget tar utgangspunkt i datalagringsdirektivet og begreper som «serious crime» (artikkel 1) og «specific cases» (artikkel 4). For det første antyder dette noe om de skranker som ligger i menneskerettighetene. For det andre er hensikten med direktivet å bekjempe alvorlig kriminalitet.

Det foreligger ikke noen omforent internasjonal forståelse av hva som er alvorlig kriminalitet, men noen folkerettslige instrumenter kan gi visse føringer. FN-konvensjonen mot grenseoverskridende organisert kriminalitet har en definisjon av «serious crime» som atferd som utgjør et lovbrudd som kan medføre frihetsberøvelse i minst fire år eller en strengere straff.

I den norske gjennomføringsbestemmelsen i straffeloven 1902 § 162 c om å inngå forbund med noen om å begå en straffbar handling, er strafferammekravet satt til fengsel i minst 3 år. Forslaget fra Justisdepartementet var imidlertid på fengsel i minst 4 år (Ot prp. nr. 62 (2002-2003) Om lov om endringer i straffeloven og straffeprosessloven mv. (lovtiltak mot organisert kriminalitet og menneskehandel, gjengangerstraff mv.) kapittel 4.5.3.1 side 27):

> «Lovutkastet omfatter bare forbund om handlinger som kan straffes med fengsel i minst 4 år. Bestemmelsen oppfyller dermed konvensjonens minimumsforpliktelse, jf. formuleringen 'agreeing … to commit a serious crime' sammenholdt med definisjonen i artikkel 2 bokstav b. Statene står imidlertid fritt til å gå lengre enn det konvensjonen krever. Hadde man fastsatt en lavere grense, slik at også forbrytelser med en strafferamme på fengsel i 3 år eller mer ble omfattet, ville det i tillegg blitt straffbart å inngå forbund om bl.a. alminnelige vinningsforbrytelser. Etter departementets oppfatning vil dette være å gå for langt, og det fremmes derfor ikke forslag om dette.»

Justiskomiteens begrunnelse for å senke strafferammekravet var som følger (Innst.O. nr. 118 (2002-2003)):

> «Flertallet ser likevel at de straffbare forhold kriminelle organiserer seg for å begå, ofte vil ha en strafferamme på 3 år, typisk tyveri etter straffeloven § 257. Det er ønskelig å harmonisere hva som anses som organisert kriminalitet i denne sammenheng i størst mulig grad med det komiteens flertall uttalte i Innst.O. nr. 73 (2002-2003) under kapittel 6.1. Derfor vil dette flertallet endre definisjonen av organisert kriminell gruppe i forslaget til straffeloven ny § 60 a annet ledd og ny §§ 162 c første ledd og annet ledd, slik at kravet til strafferamme i definisjonen reduseres fra minst 4 års fengsel til minst 3 års fengsel. Dette vil få den betydning at en vil fange opp organiserte kriminelle grupper som har som hovedformål å begå en serie av vinningsforbrytelser med strafferamme på 3 års fengsel, selv om lovteksten som sådan ikke stiller krav om at det skal begås flere handlinger.»

På europeisk plan gir rammebeslutningen om den europeiske arrestordren (2002/584/RIA) visse føringer. Artikkel 2 inneholder en liste over 32 kriminelle handlinger/handlingstyper og lemper på overleveringsvilkårene når 1) arrestordren er grunnet på en av disse handlingene, og 2) den aktuelle handlingen kan straffes med fengsel i minst tre år i staten som krever overlevering. Tanken bak unntaksbestemmelsen er at det skal gjelde lempeligere vilkår for overlevering når mistanken eller dommen som ligger til grunn for arrestordren gjelder grov, grenseoverskridende kriminalitet. Om strafferammekravet settes til mer enn tre år, vil dette i større grad reflektere skillet i norsk rett mellom simple og grove lovbrudd.

EMK forutsetter en avveining mellom personvernhensyn og behovet for lagrede data for kriminalitetsbekjempelsen. Generelt gjelder at jo mer alvorlig en handling er jo større antas behovet for å bekjempe denne type kriminalitet å være. Følgelig vil det være slik at jo høyere strafferammekrav man setter som terskel for utlevering av trafikkdata til politiet (eventuelt supplert med bestemmelser hvor det er et særskilt behov for tilgang til slike opplysninger), jo lettere vil det være å argumentere for at utleveringsadgangen er et nødvendig inngrep i personvernet.

Innhenting av data kan oppleves som relativt inngripende i forhold til den enkeltes personvern. Ved bruk av tvangsmidler som ransaking og beslag, og ikke minst pågripelse og varetektsfengsling, skjer inngrepet der og da. Jo lengre periode dataene dekker og jo lengre bakover i tid dataene er registrert, jo større blir forskjellen til eksempelvis data som kan hentes ut fra en beslaglagt mobiltelefon. På den annen side er utlevering av trafikkdata helt klart langt mindre inngripende enn kommunikasjonskontroll (vilkår om 5 eller 10 års strafferamme). Et vilkår om krav til strafferamme på fire år eller mer reflekterer etter departementets vurdering den graden av inngrep i personvernet som innhenting av data representerer.

Basestasjonssøk er mer inngripende i forhold til personvernet, blant annet fordi man da får med seg mye overskuddsinformasjon. Det tilsier strengere vilkår for utlevering av basestasjonsutskrifter enn trafikkdata. I Danmark er det et tilleggsvilkår for uthenting av denne typen data at mistanken i tillegg knytter seg til et straffbart forhold som

medfører fare for liv og helse, eller betydelige samfunnsverdier.

Innhenting av basestasjonsdata kan sammenlignes med razzia (strprl. § 194) i den forstand at bruk av tvangsmidlet vil være et inngrep i personvernet til en – potensielt lang – rekke tredjepersoner helt utenfor mistanke. Strafferammekravet for bruk av razzia er fengsel i 8 år eller mer. Det kan i så måte også sammenlignes med skjult fjernsynsovervåkning, som bare har et strafferammekrav på fengsel i mer enn 6 måneder, likevel slik at opptak av hvem som befinner seg på et bestemt sted ikke gir tilsvarende muligheter for analyse av kommunikasjon som trafikkdata gir.

Siden vilkåret for utlevering av trafikkdata settes til en strafferamme på 4 år eller mer for personspesifikke trafikkdata, foreslås således å sette strafferammekravet for uthenting av basestasjonsopplysninger til fengsel i 5 år eller mer. Dette åpner for basestasjonssøk i de fleste av de sakstypene som er nevnt over, herunder i narkotikasaker ved mistanke om grov overtredelse.

Både for utlevering av trafikkdata og for basestasjonssøk foreslås dessuten et alternativt, likelydende vilkår for handlinger som det er grunn til å tro at utøves som ledd i virksomheten til en organisert kriminell gruppe. Ved et strafferammekrav på 4 år eller mer, eventuelt 5 år eller mer for basestasjonssøk, faller for eksempel simpelt tyveri utenfor. Departementet mener imidlertid at dersom det er grunn til å tro at tyveriet (eller et annet simpelt vinningslovbrudd) er begått som ledd i virksomheten til en organisert kriminell gruppe, bør dette gi grunnlag for utlevering av trafikkdata, selv om holdepunktene for tilknytning til organisert kriminalitet ikke er så sterke at den forhøyede strafferammen som følger av straffeloven 1902 § 60 a gir grunnlag for utlevering. Derved gis det i noen grad grunnlag for utlevering av trafikkdata eller basestasjonssøk selv for handlinger med lavere strafferamme enn fengsel i henholdsvis 4 år eller mer, eller fengsel i 5 år eller mer. Behovet for tilgang til data i arbeidet med å bekjempe organisert kriminalitet er også særskilt nevnt i datalagringsdirektivets fortale (punkt 7), jf. kapittel 12.3.

I høringen ble det fra politihold advart mot å sette vilkår som i praksis bare ville la seg oppfylle ved uthenting av data. Valget av kriteriet «grunn til å tro» er gjort for å ta høyde for denne problematikken og derigjennom imøtekomme politiets behov.

I både straffeprosessloven § 210 b om trafikkdata og § 210 c om basestasjonssøk foreslås dessuten tilføyd en uttømmende oppregning av straffebud som har en lavere strafferamme enn henholdsvis 4 år eller mer eller 5 år eller mer. Felles for disse bestemmelsene er at de gjelder forhold som vil kunne være særlig vanskelige å etterforske uten tilgang til data. Generelt har en sett hen til hvilke bestemmelser som er føyd til i kapittelet om kommunikasjonskontroll i strpl kap 16 a (strpl § 216 a og 216 b).

Til straffeprosessloven § 210 b foreslås tilføyd:

- Straffeloven 1902 §§ 90, 91, 91 a, 94 jf. 90: åpenbare statshemmeligheter
- Straffeloven 1902 §§ 270 første ledd nr. 2, 145 annet ledd, 145 a, 145 b, 190 a: datakriminalitet
- Straffeloven 1902 §§ 162 og 162 b: narkotikalovbrudd, herunder doping
- Straffeloven 1902 §§ 104 a annet ledd og 162 c: danne kriminelle forbund
- Straffeloven 1902 §§ 201 a, 203, 204 a: grooming, seksuelle overgrep mot barn, barneporno
- Straffeloven 1902 § 317 jf. §§ 162: hvitvasking av utbytte fra narkotikahandel etc.
- Straffeloven 1902 § 390 a: forstyrrelse av privatlivet
- Utlendingsloven § 108 fjerde ledd: menneskesmugling

Til straffeprosessloven § 210 c foreslås tilføyd:

- Straffeloven 1902 §§ 90, 91, 91 a, 94 jf. 90: åpenbare statshemmeligheter
- Straffeloven 1902 §§ 162 og 162 b: narkotikalovbrudd, herunder doping
- Straffeloven 1902 §§ 104 a annet ledd og 162 c: danne kriminelle forbund
- Straffeloven 1902 § 317 jf. § 162: hvitvasking av utbytte fra narkotikahandel etc.
- Utlendingsloven § 108 fjerde ledd: menneskesmugling

Departementet viderefører forslaget om at det må foreligge skjellig grunn til mistanke om bestemte straffbare handlinger. Dette er gjennomgående et vilkår for bruk av straffeprosessuelle tvangsmidler i etterforskningsøyemed, og må antas å gjelde også for utlevering av data etter gjeldende regler om beslag og utleveringspålegg.

Forslaget i høringsnotatet om at kravet til skjellig grunn til mistanke må knytte til bestemte personer, er imidlertid ikke opprettholdt. Det vil innebære en for stram begrensning på bruken av data.

Man kan eksempelvis tenke seg at flere er mistenkt i saken, uten at det foreligger skjellig grunn til mistanke mot noen av dem. Dette bør ikke være til hinder for innhenting av data, så fremt det

foreligger skjellig grunn til mistanke om en så vidt alvorlig straffbar handling som det er snakk om her, og såfremt dataene antas å være av vesentlig betydning for saken, jf. nedenfor. I forhold til basestasjonssøk ville et slikt vilkår i praksis frata politiet muligheten for innhenting av slike opplysninger til bruk i etterforskningen. For eksempel vil et krav om en navngitt mistenkt blant annet stenge for utlevering av data i saker med kjent offer og ukjent gjerningsperson, og hvor innhenting av basestasjonsutskrifter typisk er aktuelt.

Flere høringsinstanser – Riksadvokaten, Det nasjonale statsadvokatembetet og Politiets Fellesforbund – nevner lovfesting av et krav om at dataene må være av vesentlig betydning for etterforskningen som et alternativ til kravet om at mistanken må rettes mot en bestemt person. En slik innskjerping av kravet til trafikkdataenes antatte bevisverdi har gode grunner for seg. Det skal sikre at utlevering av data bare pålegges i tilfellet hvor dataene må antas å være av stor betydning for etterforskningen og derfor er et nødvendig inngrep i personvernet. Retten må dermed foreta en konkret, rimelig avgrensning av utleveringsbegjæringen og i sin kjennelse både foreta avgrensninger i tid, sted og i forhold til personer. I saker med kjent gjerningsperson vil retten kunne tillate at det hentes inn data om andre enn mistenkte så fremt det er av vesentlig betydning for etterforskningen og øvrige vilkår er oppfylt. Dette kan medføre en endring fra dagens praksis hvor Post- og teletilsynet i liten grad har åpnet for å innhente data om andre enn den som er mistenkt.

Den generelle forholds- og hensiktsmessighetsvurderingen som skal foretas ved bruk av ethvert tvangsmiddel etter straffeprosessloven fjerde del, kommer også til anvendelse ved utlevering av data, jf. *straffeprosessloven § 170 a*. I dette ligger at domstolen må foreta en konkret vurdering av utleveringsbegjæringen opp mot blant annet alternative, mindre inngripende tvangsmidler. I vurderingen av om inngrepet vil være uforholdsmessig vil dessuten personvernhensynene måtte vektlegges. Relevante momenter her er hvor lang tid tilbake begjæringen gjelder for, hvor alvorlig den konkrete straffbare handlingen er, men også hvor avgjørende dataene er for etterforskningen. Man kan eksempelvis tenke seg at strafferammekravet i og for seg er oppfylt, men at domstolen likevel kommer til at den konkrete handlingen ikke er så alvorlig at den forsvarer utlevering av trafikkdata som begjært. Det kan også være at domstolen velger å korte ned på hvor lang tid tilbake data skal kunne utleveres for etter en avveining av personverninngrepet vurdert opp mot handlingens konkrete alvorlighet og dataenes antatte betydning for etterforskningen. Motsatt: Er det snakk om en drapsetterforskning, er det vanskelig å tenke seg at utlevering kan være uforholdsmessig hvis først vilkårene for utlevering er oppfylt. Men også her må det vurderes hvor langt tilbake i tid det er grunn til å gå. Andre avgreningsmuligheter er å begrense antall personer det skal innhentes data om, eller tids- og stedsavgrensning for så vidt gjelder basestasjonssøk.

Utlevering av trafikkdata og lokaliseringsdata i forbindelse med straffesaker skal underlegges *domstolskontroll*. Dette er i samsvar med forslaget i høringsnotatet og fikk bred støtte under høringen.

Departementet foreslår videre at dagens ordning med at påtalemyndigheten har hastekompetanse videreføres. Høringen bekrefter at det i tillegg til domstolenes primærkompetanse er behov for slik hastekompetanse for påtalemyndigheten i tilfeller hvor etterforskningshensyn tilsier at innhenting ikke kan vente til rettens kontortid.

Forslaget til ny bestemmelse om utlevering av trafikkdata er i realiteten en lovfesting av vilkår som i stor grad gjenspeiler den type momenter som Post- og teletilsynet har lagt vekt på i forbindelse med begjæringer om opphevelse av taushetsplikten etter straffeprosessloven § 118 første ledd. Under høringen har blant andre Telenor stilt spørsmål ved om ikke Post- og teletilsynet fortsatt bør ha en rolle i forbindelse med domstolsbehandling av en begjæring om utlevering av trafikkdata, blant annet for å kunne avveie hensynene til henholdsvis kriminalitetsbekjempelse og personvern. Departementet bemerker til dette at det etter lovforslaget skal være domstolen som avveier disse hensynene mot hverandre og det er ikke naturlig at et tilsynsorgan skal overprøve denne beslutningen. Post- og teletilsynet skal dermed ikke lenger ha en rolle i forbindelse med opphevelse av taushetsplikten i saker hvor utleveringspålegget er truffet av retten. Det samme skal gjelde i saker hvor utleveringspålegg er fattet av påtalemyndigheten med hjemmel i bestemmelsen om hastekompetanse.

Beslutning om utlevering av data skal etter forslaget skje ved kjennelse og således begrunnes. Retten skal sørge for at den som rammes snarest mulig blir kjent med kjennelsen, jf. straffeprosessloven § 52 annet ledd. På samme måte som ellers ved ransaking, beslag og utleveringspålegg, bør det imidlertid være hjemmel også her for utsatt underretning når dette er strengt nødvendig for etterforskningen. Slik utsatt underretning kan

være særlig aktuelt i de tilfellene hvor dataene søkes innhentet i en tidlig fase av etterforskningen og før det er foretatt noen pågripelse. Blir den som i slike tilfeller rammes, klar over utleveringspålegget, kan det ofte miste mye av sin effekt. Videre etterforskning, eksempelvis ransaking og beslag, kan dessuten bli vanskeliggjort.

For å bøte på manglende kontradiksjon i slike tilfeller bør det, som ved utsatt underretning om ransaking mv., oppnevnes offentlig advokat for mistenkte. Det foreslås derfor at forslaget til ny § 210 d om utsatt underretning i saker om utlevering av data etter straffeprosessloven § 210 b og § 210 c, føyes til i listen over sakstyper i straffeprosessloven § 100 a første ledd.

13 Utlevering av data i avvergende og forebyggende øyemed

13.1 Gjeldende rett

Utlevering av data til politi og påtalemyndighet etter straffeprosessloven §§ 210 b og c skal skje som ledd i etterforskningen av mulige straffbare forhold. Straffeprosessloven kapittel 17 b åpner i tillegg for at politi og påtalemyndighet kan gis tillatelse til å anvende tvangsmidler for å innhente informasjon med sikte på å *avverge* noen bestemte former for organisert og annen alvorlig kriminalitet, jf. straffeloven 1902 § 222 d første ledd. Retten kan bare gi tillatelse til bruk av tvangsmidler med hjemmel i § 222 d der bruken vil skje som ledd i etterforskning og det er «rimelig grunn til å undersøke» om det foreligger en handling som rammes av et av aktuelle straffebudene. Endelig stiller § 222 d tredje ledd som vilkår at det antas at «inngrepet vil gi opplysninger av vesentlig betydning» for å kunne avverge handlingen saken gjelder og at avvergingen ellers «i vesentlig grad vil bli vanskeliggjort».

Tillatelsen skal normalt gis av retten, som treffer sin avgjørelse ved kjennelse. Tilsier behovet for avvergelse at innhenting ikke kan vente til rettens kontortid kan ordre fra påtalemyndigheten likevel tre i stedet for kjennelse fra retten. Rettens godkjennelse skal innhentes snarest mulig og senest innen 24 timer etter at tvangsmidlet ble tatt i bruk.

Politiets sikkerhetstjeneste (PST) har i medhold av straffeprosessloven § 222 d annet ledd adgang til å få utlevert data i avvergende øyemed i saker som gjelder overtredelse av noen flere straffebud enn etter første ledd.

Politiloven § 17 d første og annet ledd åpner for at retten ved kjennelse kan gi PST tillatelse til bruk av tvangsmidler i *forebyggende* øyemed, det vil si utenfor etterforskning. Handlingen ligger da lenger frem i tid enn i tilfeller hvor det er snakk om tvangsmiddelbruk i avvergende øyemed. Politiloven § 17 d tredje ledd gir PST på nærmere bestemte vilkår hastekompetanse med etterfølgende domstolskontroll.

13.2 Høringsnotatet og høringsinstansenes syn

I *høringsnotatet* ble det lagt til grunn at i den grad politi og påtalemyndighet har behov for utlevering av lagrede data i avvergende øyemed, ville dette reguleres av straffeprosessloven § 222 d. Politiloven § 17 d om tvangsmiddelbruk i forebyggende øyemed ble ikke omtalt her.

Oslo statsadvokatembeter etterlyser en omtale av politiloven § 17 d og bemerker at dersom lagringstiden utvides vesentlig utover seks måneder, vil PST gis et dramatisk økt og lett tilgjengelig datatilfang.

13.3 Departementets vurdering

Departementet foreslår ingen endring i straffeprosessloven § 222 d om politi og påtalemyndighets bruk av tvangsmidler i avvergende øyemed. Henvisningen her til straffeprosessloven kapittel 16 innebærer at utlevering av trafikkdata også i fremtiden vil kunne nyttes i avvergende øyemed, forutsatt at vilkårene for slik tvangsmiddelbruk er oppfylt.

Departementet foreslår heller ingen endring i politiloven § 17 d om tvangsmidler som er tilgjengelig for PST i forebyggende øyemed.

Det er korrekt, som påpekt av Oslo statsadvokatembeter, at utvidelsen av lagringstiden for data omfattet av direktivet vil ha betydning for omfanget av data som hjemlene om tvangsmidler i avvergende og forebyggende øyemed åpner for. Departementet vil samtidig understreke at begge disse hjemlene er snevre og at lovforslaget ikke innebærer noen endring av vilkårene for inngrepet. Ordningen med domstolskontroll består uendret. Selv om lagringstiden øker, er dette ikke ensbetydende med at større mengder data vil bli utlevert i den enkelte sak. Eksempelvis kan vesentlighetskravet i straffeprosessloven § 222 d tredje ledd først punktum og i politiloven § 17 d annet ledd første punktum kunne være til hinder for dette.

Metodekontrollutvalget har i NOU 2009: 15 foreslått endringer i straffeprosessloven § 222 d (utredningen kapittel 2.4 side 24):

> «I dag krever straffeprosessloven § 222 d at avvergende tvangsmiddelbruk må skje 'som ledd i etterforsking', det vil si at det må være grunn til å tro at noen er i ferd med å begå eller har begått en straffbar handling. Det kreves imidlertid ingen sammenheng mellom den handlingen etterforskingen opprinnelig var rettet mot, og den handlingen som søkes avverget. Utvalget foreslår at det må kreves både rimelig grunn til å tro at noen kommer til å begå en nærmere bestemt, svært alvorlig handling, og at de 'som ledd i forberedelsen' allerede har begått en straffbar handling som kan medføre fengselsstraff. Det innebærer et krav om tydeligere sammenheng mellom den forbrytelse som søkes avverget og en allerede begått straffbar handling.»

Lovforslaget vil bli vurdert i forbindelse med oppfølgningen av Metodekontrollutvalgets utredning som Justisdepartementet nå arbeider med.

13.4 Straff for brudd på tilbyders taushetsplikt ved utlevering i forebyggende øyemed

Enhver som utfører arbeid eller tjeneste for påtalemyndigheten er underlagt taushetsplikt med hensyn til hva vedkommende i straffesaker får kjennskap til om noens personlige forhold eller tekniske innretninger, jf. straffeprosessloven § 61. Politi og påtalemyndighet har dessuten adgang til å pålegge tilbydere av elektroniske kommunikasjonstjenester taushetsplikt om det tilbyderne får kjennskap til i forbindelse med at de bistår politi eller påtalemyndighet, jf. straffeprosessloven § 61 c siste ledd første punktum. Overtredelse av slike pålegg kan straffes etter straffeloven 1902 § 121 dersom tilbyder er gjort oppmerksom på dette, jf. siste punktum.

Politiloven § 17 d pålegger enhver, også tilbydere, å bevare taushet om at det er begjært eller besluttet bruk av tvangsmidler i forebyggende øyemed etter § 17 d. Straffeloven 1902 § 121 rammer i utgangspunktet ikke andre enn de som krenker taushetsplikt som følger av «tjeneste eller arbeid for statlig eller kommunalt organ». Dette er endret i straffeloven 2005 § 209 som rammer ethvert brudd på taushetsplikt så fremt plikten følger av lov eller forskrift. Brudd på pålagt taushetsplikt vil også rammes av straffeloven 1902 § 121 i medhold av politiregisterloven § 35.

Metodekontrollutvalget har i NOU 2009: 15 foreslått at det tas inn en henvisning i politiloven § 17 f til straffeloven 1902 § 121 lik den som finnes i straffeprosessloven § 61 c siste ledd siste punktum. Etter utvalgets oppfatning er det ingenting som tilsier at brudd på taushetsplikten etter § 17 f ikke bør få samme konsekvenser for alle involverte.

I *høringsnotatet* ble denne problemstillingen løftet frem, bl.a. i form av følgende sitat fra utvalgets utredning (kapittel 20.5 side 221):

> «Selv om 'alle' vil ha taushetsplikt om dette etter politiloven § 17 d, jf. § 17 f, 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 § 17 f ikke bør få samme konsekvenser for alle involverte, og utvalget foreslår derfor at det tas inn en henvisning i politiloven § 17 f til straffeloven § 121 lik den som finnes i straffeprosessloven § 61c siste ledd siste punktum.»

Politiets sikkerhetstjeneste støtter forslaget:

> «Høringsnotatet viser […] til behovet for taushet i forbindelse med benyttede tvangsmidler. For PST gjelder behovet for at alle involverte bevarer taushet også når det benyttes tvangsmidler — herunder innhenting av trafikkdata — i forebyggende saker. Det vises til at Metodekontrollutvalget foreslår en hjemmel til å ilegge straffesanksjonert taushetsplikt for forebyggende tvangsmidler ved en endring i politiloven § 17 f. PST anmoder om at denne endringen gjøres i forbindelse med innføring av lagringsplikt for trafikkdata, da det særlig er i forbindelse med teletilbydernes utlevering av trafikkdata det har vist seg å være behov for en slik bestemmelse.»

Departementet ser det som inkonsekvent at tilbyders brudd på taushetsplikten kan straffes dersom taushetsplikten gjelder opplysninger gitt i avvergende øyemed, men ikke om de er gitt i forebyggende øyemed. At taushetsplikten overholdes, og at brudd kan sanksjoneres, er svært viktig i begge tilfeller og både av hensyn til kriminalitetsbekjempelse og av hensyn til personvernet for de

som rammes. Departementet følger derfor opp Metodekontrollutvalgets forslag om et tillegg i politiloven § 17 f om straff etter straffeloven 1902 § 121 ved brudd på taushetsplikten etter politiloven § 17 d. Tillegget vil bli overflødig når politiregisterloven og straffeloven 2005 trer i kraft.

14 Regler for tilgang til data for andre

14.1 Innledning

Adgangen til å hente ut data som er lagret i henhold til direktivet, er regulert i datalagringsdirektivet artikkel 4. Herav følger at data bare skal utleveres til kompetente nasjonale myndigheter i særlige saker og i overensstemmelse med nasjonal lovgivning. Det fremgår videre at hver medlemsstat skal fastsette hvilke prosedyrer som skal følges, og hvilke betingelser som skal være oppfylt for å få adgang til lagrede data i overensstemmelse med kravet om nødvendighet og proporsjonalitet.

Departementet mener som altoverveiende hovedregel at bare politi og påtalemyndighet skal være kompetent myndighet for uthenting av data som er lagret i medhold av direktivet. Dette er en naturlig konsekvens av at siktemålet med datalagringsdirektivet er å bekjempe kriminalitet og at denne oppgaven primært påligger politi og påtalemyndighet.

Det er likevel et spørsmål om det kan være spesielle grunner som taler for å åpne for utlevering til andre enn politiet. Dette behandles i det følgende.

14.2 Gjeldende rett

14.2.1 Om andre myndigheters tilgang

Ekomloven § 2-9 fastsetter taushetsplikt ved bruk av elektronisk kommunikasjon, og gjelder både tilbyder av elektronisk kommunikasjonsnett- eller tjeneste og personer som utfører arbeid eller tjeneste for slik tilbyder, jf. henholdsvis første og annet ledd. Taushetsplikten omfatter innholdet av kommunikasjonen og andres bruk av elektronisk kommunikasjon. Begrepet «bruk» knytter seg til alle sider av et abonnementsforhold for elektronisk kommunikasjon, og innebærer blant annet at trafikkdata, opplysninger om basestasjonstilknytning (lokaliseringsdata), tidspunkt for på- og avlogging av internett- eller e-posttjeneste samt abonnents/brukerdata anses som en del av det taushetsbelagte materiale.

Utlevering bare kan skje med hjemmel i lov. Bestemmelsene i § 2-9 tredje ledd innskrenker og opphever taushetsplikten i visse tilfeller. I henhold til tredje ledd første punktum er taushetsplikten ikke til hinder for at det gis opplysninger til påtalemyndigheten eller politiet om avtalebasert hemmelig telefonnummer eller andre abonnementsopplysninger, samt elektronisk kommunikasjonsadresse. Slike opplysninger kan også gis ved vitnemål for retten, jf. tredje ledd annet punktum. Bestemmelsen omfatter kun identifikasjonsdata, og hjemler ikke utlevering av trafikkdata eller lokaliseringsdata.

Andre offentlige myndigheter enn politi og påtalemyndighet kan bare innhente opplysninger fra tilbyder om lagrede data dersom det finnes lovhjemmel som gjør unntak fra taushetsplikten i § 2-9, jf. tredje ledd tredje punktum. Innhentingen skjer da ikke som ledd i en straffesak, men er et tiltak administrative myndigheter foretar som ledd i sin alminnelige kontroll med at lovgivningen på et bestemt område blir overholdt. Omfanget av opplysningsplikten i slike tilfeller vil framgå av vedkommende hjemmelslov.

Den adgang enkelte myndighetsorganer i henhold til lovgivningen har til å innhente visse opplysninger fra ekomtilbydere er i de fleste tilfeller begrenset til å gjelde abonnements- og brukerdata omhandlet i tredje ledd første punktum. Slik hjemmel finnes i dag i tolloven § 12-4 første ledd, merverdiavgiftsloven § 16-3 og ligningsloven § 6-13a, som alle åpner for at kontrollmyndighetene kan pålegge tilbyder å gi opplysninger om navn og adresse til en abonnent som ikke har offentlig telefonnummer eller telefaksnummer (eller personsøkernummer). Det er et vilkår at særlige hensyn gjør det nødvendig, og at det foreligger mistanke om overtredelse av bestemmelser gitt i eller i medhold av henholdsvis ligningsloven, merverdiavgiftsloven og tolloven. I Ot.prp. nr. 21 (1999-2000) Endringer i skatteloven mv. som ligger til grunn for hjemlene, drøftet departementet uttrykkelig hvorvidt kontrollmyndighetene skulle få adgang til å innhente abonnement/brukerdata også ved andre kommunikasjonsformer, men konkluderte benektende, jf. proposisjonen s. 38. Det må derfor legges til grunn at kontrollmyndighetene ikke har adgang til å kreve utlevert abon-

nent/brukerdata knyttet til en dynamisk IP-adresse. Finanstilsynet har imidlertid en videre adgang til å innhente abonnement/brukerdata i medhold av verdipapirhandelloven § 15-3 annet ledd nr. 2, som åpner for at «opplysninger om avtalebasert hemmelig telefonnummer eller andre abonnementsopplysninger og elektronisk kommunikasjonsadresse» kan innhentes uavhengig av taushetsplikten i ekomloven § 2-9. Vilkåret er at det foreligger mistanke om overtredelse av nærmere angitte bestemmelser i verdipapirlovgivningen. I slike tilfeller må Finanstilsynet antas å kunne få utlevert alle typer opplysninger omfattet av ekomloven § 2-9 tredje ledd første punktum.

Finanstilsynet er eneste offentlig organ i Norge utenom politi og påtalemyndighet som er gitt kompetanse til å innhente trafikkdata, jf. verdipapirhandelloven § 15-3 annet ledd nr. 3. Bestemmelsen gjennomfører EØS-forpliktelser som følger av direktiv 2003/6/EF om markedsmisbruk (markedsmisbruksdirektivet) artikkel 12 nr. 2 bokstav d og direktiv 2004/39/EF om markeder for finansielle instrumenter (MiFID) artikkel 50 nr. 2 bokstav d. Bestemmelsen stiller uttrykkelig krav om forutgående opphevelse av taushetsplikten for at trafikkdata skal kunne utleveres. Samtykkekompetansen ligger i utgangspunktet hos departementet, men er delegert til Post- og teletilsynet. Ved vurderingen av om fritak skal gis skal det blant annet legges vekt på hensynet til taushetsplikten og sakens opplysning, jf. bestemmelsens tredje punktum.

Finanstilsynets hjemmel til å hente ut trafikkdata har av ulike grunner ikke vært operativ, jf. beskrivelsen i Ot.prp. nr. 34 (2006-2007) Om lov om verdipapirhandel (verdipapirhandelloven) og lov om regulerte markeder (børsloven) s. 259-260. Bakgrunnen for dette er blant annet at det har hersket tvil om hvilke saksbehandlingsregler som gjelder ved Finanstilsynets anmodning om opphevelse av taushetsplikten. Etter det departementet kjenner til, har Post- og teletilsynet aldri opphevet taushetsplikten etter anmodning fra Finanstilsynet. Paragraf 15-3 annet ledd nr. 3 fjerde punktum inneholder en forskriftshjemmel som skulle legge til rette for å få på plass forsvarlige saksbehandlingsregler. Finansdepartementets sendte ut et høringsbrev 18. desember 2007 vedrørende forslag til forskriftsbestemmelser om saksbehandlingsreglene for Kredittilsynets innhenting av trafikkdata. Behandlingen av høringsforslaget er imidlertid utsatt av hensyn til implementeringen av datalagringsdirektivet.

Videre finnes det mer generelle lovhjemler for andre offentlige kontrollorganer til å innhente opplysninger uavhengig av taushetsplikt. Folketrygdloven § 21-4 a tredje ledd er et eksempel på en generell hjemmel til å kreve opplysninger eller innsyn i dokumenter mv. uten hinder av taushetsplikt. Etter folketrygdloven § 21-4 a første ledd kan slike opplysninger utleveres når det foreligger rimelig grunn til mistanke om urettmessige utbetalinger fra trygden. Det er ikke etablert en sikker forståelse av om folketrygdloven § 21-4 a og lignende, mer generelle bestemmelser om kontrollmyndigheters informasjonsinnhenting etablerer en lovhjemmel som forutsatt i ekomloven § 2-9 tredje ledd om utlevering av abonnement/brukerdata.

14.2.2 Om utlevering av lagrede data som bevis i sivile saker

Tvisteloven § 22-3 inneholder bestemmelser om bevisforbud om opplysninger undergitt lovbestemt taushetsplikt, herunder opplysninger som «tilbyder eller installatør av elektronisk kommunikasjonsnett eller tjeneste» har. For at abonnement/brukerdata, trafikkdata og lokaliseringsdata skal kunne anvendes som bevis for retten, må taushetsplikten oppheves av Post- og teletilsynet (etter kompetanse delegert fra departementet). Samtykke kan bare nektes når bevisføring kan utsette staten eller allmenne interesser for skade eller virke urimelig overfor den som har krav på hemmelighold, jf. bestemmelsens annet ledd annet punktum. I tredje ledd første punktum er retten gitt kompetanse til å overprøve samtykke eller nektelse av å gi samtykke etter annet ledd. Retten skal her foreta en selvstendig avveining mellom hensynet til taushetsplikten og hensynet til sakens opplysning.

Av Høyesteretts kjennelse 18. juni 2010 (Altibox) følger at tvisteloven § 22-3 annet og tredje ledd skal gis tilsvarende anvendelse ved bevissikring utenfor rettssak, jf. tvisteloven kapittel 28. Kjennelsen er inntatt i Rt. 2010 s. 774. Det vil særlig kunne være relevant å innhente data før det er tatt andre rettslige skritt i de tilfellene der trafikkdata er avgjørende for å bringe på det rene identiteten til personer, som det kan være aktuelt å rette et sivilrettslig krav mot. I den konkrete sak ble en internettleverandør pålagt å opplyse om identiteten til en abonnent ettersom det var anført at abonnenten ved ulovlig fildeling hadde brutt bestemmelser i åndsverksloven.

14.3 Høringsnotatets forslag

I høringsnotatet la departementene til grunn at lagrede opplysninger som det klare utgangspunkt bare skulle kunne utleveres til politi og påtalemyndighet. Departementene trakk likevel et skille mellom trafikkdata og lokaliseringsdata på den ene side, og abonnements- og brukerdata på den annen side.

For så vidt gjelder abonnements- og brukerdata foreslo departementene å videreføre gjeldende rett, hvoretter utlevering til sivile myndigheter kan skje uhindret av taushetsplikten der dette er særskilt hjemlet i lov. Etter forslaget skulle utlevering av trafikk- og lokaliseringsdata forbeholdes politi- og påtalemyndigheten. Det ble vist til at 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. Det ble også vist til at det heller ikke i dag er adgang for andre myndigheter enn politiet til å bruke tvangsmidler etter straffeprosessloven som ledd i en straffesak. Departementene holdt imidlertid åpent hvorvidt Finanstilsynets tilgang til trafikkdata etter verdipapirhandelloven § 15-3 annet ledd nr. 3 burde videreføres.

Tvisteloven § 22-3 – som åpner for at bevis omfattet av ekomlovens taushetspliktregler føres i sivil rettergang – ble foreslått videreført uendret. Departementene gikk inn for at Post- og teletilsynet fortsatt skulle vurdere spørsmålet om samtykke til opphevelse av taushetsplikten før retten skal kunne tillate at trafikkdata fremlegges som bevis i sivile søksmål.

14.4 Høringsinstansenes syn

Finansdepartementet, Politidirektoratet, Finanstilsynet, Post- og teletilsynet, NorSIS, Telenor, Ventelo, NetCom, NextGenTel, NHO, IKT-Norge, Teknologirådet, TEKNA, ITAKT, NITO, UiO, og *Elektronisk Forpost Norge* har problematisert forholdet om hvem som skal ha tilgang til data som er lagret i medhold av datalagringsdirektivet. De fleste høringsinstanser som har uttalt seg om dette, deler oppfatningen om at adgangen bør begrenses, og mener at det kun er politi og påtalemyndighet som bør få tilgang til disse data. Mange av de samme høringsinstansene frykter at det på sikt vil skje en formålsutglidning, slik at flere og flere myndigheter vil kunne få tilgang til lagrede data. Videre mener de fleste som har uttalt seg om dette, at dersom Finanstilsynet fortsatt skal ha tilgang til trafikkdata må de samme vilkårene for tilegnelsen gjelde som for politi- og påtalemyndighet.

14.4.1 Om andre myndigheters tilgang

Post- og teletilsynet viser i høringen til at høringsnotatet bare nevner Finanstilsynet som myndighet med hjemmel for tilgang. Post- og teletilsynet mener at flere andre myndigheter kan ha tilgang gjennom sitt regelverk og nevner NAV og Havarikommisjonen. Tilsynet mener at tilgangen bør begrenses og at det bør kreves eksplisitt lovhjemmel. Videre bør tilgangen for andre prosessuelt være lik politiets. *Post- og teletilsynet* uttaler:

> «Generelt mener PT at tilgangen til trafikkdata bør begrenses til de tilfeller hvor fordelene med å få tilgang til trafikkdata for mottakende etat klart overstiger de personvernmessige konsekvensene. Denne vurderingen bør gjøres konkret og individuelt. Etter Post- og teletilsynets syn bør det derfor kreves eksplisitt lovhjemmel hvis en etat skal få tilgang til trafikkdata.»

Finansdepartementet mener at Finanstilsynet bør ha tilgang til trafikkdata og begrunner dette slik:

> «Finanstilsynets hjemmel til å innhente trafikkdata har vært lovfestet i norsk rett siden 2005, jf. verdipapirhandelloven 1997 (lov 19. juni 1997 nr. 79) § 12-2a og gjeldende verdipapirhandellov 15-3. Finanstilsynets hjemmel til å innhente trafikkdata er vedtatt av Stortinget og gjennomfører EØS-forpliktelser, jf. nedenfor. Finansdepartementet finner det uheldig at det i høringsnotatet åpnes for å revurdere hjemmelen. Finansdepartementet kan heller ikke se at spørsmålet om en eventuell implementering av datalagringsdirektivet i norsk rett gjør dette nødvendig eller ønskelig.»

Flere av tilbyderne, herunder *Telenor* og *NextGentel* mener at tilgangen bør begrenses til politiet. *NetCom* kjenner til at NAV har bedt om utlevering med hjemmel gjennom folketrygdloven, og frykter at også andre myndigheter vil kunne hevde å ha adgang til data gjennom sitt regelverk. *UiO – senter for menneskerettigheter* mener at en fragmentarisk tilgang til data for andre myndigheter kan være problematisk i forhold til lovskravet i EMK art 8(2). De peker også på at Finanstilsynets tilgang ikke er underlagt en drøftelse av nødven-

dighetskriteriet etter EMK art 8. Også *IKT-Norge* er svært skeptisk til å gi Kredittilsynet (nå Finanstilsynet) eller andre offentlige etater tilgang til data.

Politidirektoratet uttaler følgende:

> «Formålet med direktivet er å bekjempe kriminalitet og dette er en oppgave for politi og påtalemyndighet. Politidirektoratet, i likhet med Nord-Trøndelag politidistrikt, ser dette som et viktig prinsipp som ikke må uthules ved at man gir andre tilsynsorganer tilgang til data på samme måte som for politi og påtalemyndighet.»

De fleste høringsinstanser som har uttalt seg om spørsmålet om hvilke saksbehandlingsregler som bør gjelde for andre myndigheters eventuelle tilgang til data, mener at myndigheten må undergis de samme vilkår for tilegnelsen som politiet.

Post- og teletilsynet uttaler:

> «Videre mener PT at andre offentlige etaters tilgang, både materielt og prosessuelt, mest mulig bør være like den tilgang politiet får. Dette innebærer at en annen instans enn etaten selv bør godkjenne tilgangen og at tilgangen bør begrenses til alvorlige saker. Konkret innebærer dette blant annet at forsterket innsynsrett ikke bør tillates. PT anbefaler at en legger opp til tilsvarende prosessuell behandling av slike saker som for politiets tilgang.»

Finansdepartementet og *Finanstilsynet* mener at en innskrenkning eller oppheving av tilsynets tilgang til data vil innebære et brudd på internasjonale forpliktelser:

> «Det følger av EØS-forpliktelser som tilsvarer både markedsmisbruksdirektivet (direktiv 2003/6/EF) art. 12 nr. 2 bokstav d og verdipapirmarkedsdirektivet 'MiFID' (direktiv 2004/39/EF) art. 50 nr. 2 bokstav d, at kompetent myndighet skal ha tilgang til trafikkdata etter de to direktivene. Finanstilsynet er kompetent myndighet i Norge i henhold til de to nevnte direktivene. Det er derfor etter Finansdepartementets syn ikke grunn til å stille 'spørsmål ved hvordan Kredittilsynets (Finanstilsynets) tilgang til trafikkdata passer inn i det regime som vil gjelde for politiets tilgang ved innføring av regler som foreslått i dette høringsnotatet', slik departementene gjør i høringsnotatet. Det kan synes som at man i høringsnotatet ikke tar hensyn til EØS-forpliktelsene nevnt over, i og med at disse forpliktelsene ikke er nevnt eller drøftet nærmere i høringsnotatet. Etter Finansdepartementets syn vil en innskrenkning eller oppheving av Finanstilsynets tilgang til trafikkdata etter verdipapirhandelloven innebære brudd på EØS-forpliktelser som tilsvarer markedsmisbruksdirektivet og MiFID.»

Samtidig er begge positivt innstilt til å innføre domstolskontroll med utlevering av trafikkdata til tilsynet. *Finanstilsynet* skriver:

> «I høringsnotatet punkt 14.3. gjør departementene oppmerksom på at regelverket for Finanstilsynets tilgang til trafikkdata ikke forutsetter at retten har truffet avgjørelse om utlevering slik det nå foreslås for politiets tilgang til data. […] Finanstilsynet viser til at på samme måte som det foreliggende forslag til forskriftsregler om Finanstilsynets tilgang til trafikkdata inneholder saksbehandlingsregler som ligger tett opp til de straffeprosessuelle regler, vil verdipapirhandellovens hjemmelsgrunnlag og tilhørende forskriftsregler kunne tilpasses nye regler som måtte komme i og med gjennomføringen av datalagringsdirektivet. Det vises i den forbindelse til at det så vel i markedsmisbruksdirektivet og MiFID åpnes for at et tilsynsorgans kompetanse til å innhente trafikkdata kan være betinget av at en domstol treffer en rettslig avgjørelse. Tilsvarende kan det legges opp til at Finanstilsynets tilgang til trafikkdata er avhengig av rettslig kjennelse. Rettslig kjennelse er i dag et vilkår for Finanstilsynets adgang til å foreta bevissikring etter vphl. § 15-5 når det er rimelig grunn til å anta at atferdsregler i verdipapirhandellovens kapittel 3 er overtrådt, eller det er nødvendig for å oppfylle Norges avtaleforpliktelser overfor en annen stat. Finanstilsynet er også kjent med at enkelte andre EØS-land har ordninger hvor domstolsavgjørelse er et vilkår for utlevering av trafikkdata.»

14.4.2 Om utlevering av lagrede data som bevis i sivile saker

Enkelte høringsinstanser har uttalt seg om reglene i tvisteloven som gir grunnlag for at data under visse forutsetninger kan tillates innhentet til bruk som bevis i sivilrettslige søksmål. *IKT-Norge* etterlyser i sin høringsuttalelse en utredning av private aktørers mulighet for tilgang til data gjennom tvisteloven. *Norsk Videogramforening* foreslår at det klargjøres i ekomloven § 2-9

eller forarbeidene til denne, at dagens regler om tilgang til informasjon om kopling mellom sluttbrukers identitet og den IP-adressen som er anvendt, fortsatt skal gjelde. Samme høringsinstans ber om at dette klargjøres både for tilbyders tilgang (§ 2-9 første ledd), for politiets tilgang (§ 2-9 tredje ledd) og for rettighetshavers tilgang gjennom sivilrettslige søksmål (tvisteloven § 22-3) og mener at det uavhengig av implementering av direktivet bør innføres en plikt for tilbyder til å lagre «denne koplingen» i betydelige lenger tid enn de tre ukene som tillates i dag (jf. Datatilsynets konsesjoner). *Datatilsynet* er bekymret for de ulemper det kan ha for personvernet at data kan tilflyte samfunnet som følge av utlevering av data i sivile saker.

14.5 Departementets vurdering

14.5.1 Om andre myndigheters tilgang

Departementet fastholder det prinsipielle utgangspunkt at etterforskning av lovbrudd tilligger politi- og påtalemyndigheten, og ikke forvaltningen. Det er således ikke aktuelt å åpne opp for at andre myndigheter skal få tilgang til trafikkdata eller lokaliseringsdata. Av hensyn til internasjonale forpliktelser gjøres det imidlertid et unntak for Finanstilsynet for så vidt gjelder trafikkdata, jf. nedenfor under kapittel 14.5.2. Drøftelsen her dreier seg om hvorvidt andre myndigheter bør få tilgang til *abonnements-/brukerdata* og eventuelt på hvilke vilkår.

Abonnements-/brukerdata er opplysninger som er nødvendige for å knytte en bestemt abonnent til et telefonnummer eller til en IP-adresse. Opplysningene indikerer hvem som står bak en kommunikasjon, for eksempel hvem som har sendt en e-post eller foretatt en oppringning. I slike tilfeller vil den rettshåndhevende myndighet allerede være i besittelse av et elektronisk spor i form av et telefonnummer eller en IP-adresse, og en påfølgende utlevering av identifiseringsopplysninger knytter en registrert bruker til et bestemt tilfelle av elektronisk kommunikasjon.

Tilbyderne registrerer i stor utstrekning abonnements/brukerdata også i dag. Etter ekomforskriften § 6-2, jf. ekomloven § 2-8, har tilbyder av telefontjeneste plikt til å føre oversikt over enhver sluttbrukers navn, adresse og nummer/adresse for tjenesten. Oversikten skal inneholde opplysninger som gjør det mulig entydig å identifisere de registrerte. Det kan trolig ikke utledes noen plikt for tilbydere av internettaksess til å identifisere sine abonnenter etter ekomloven § 2-8. Likevel vil tilbyderne som regel sitte på et abonnementsregister som inneholder informasjon som blir registrert av tilbyderen når abonnementsforholdet opprettes. Et slikt register inneholder vanligvis blant annet abonnentens navn og adresse og teknisk informasjon om abonnementet. Slik informasjon er det normalt nødvendig for leverandøren å beholde så lenge et abonnement er aktivt. Det nye med direktivet er at slik lagring – også for nettilbydere – i fremtiden skal være en lovpålagt plikt i den hensikt at dataene skal kunne benyttes i kriminalitetsbekjempelse.

For telefoni er abonnementsopplysninger åpent tilgjengelige via tjenester som telefonkatalogen, med mindre brukeren har hemmelig nummer. Det samme er ikke tilfelle ved bruk av Internett, idet mange internettilbydere i dag benytter dynamiske IP-adresser. Hver tilbyder disponerer et visst antall IP-adresser som lånes ut til abonnentene. Dette kan skje på permanent basis (faste IP-adresser) eller dynamisk, der abonnentene tildeles en IP-adresse hver gang oppkoblingen skjer mot tilbyderen. Bakgrunnen for bruk av dynamiske IP-adresser er primært at tilbyderne har flere abonnenter enn IP-adresser eller for øvrig er nødt til å økonomisere med IP-adressene sine. Brukere som har behov for kontinuerlig nettilgang, for eksempel bedrifter, vil gjerne ha en fast linje, hvilket innebærer at de stort sett benytter den samme IP-adressen gjennom abonnementsforholdet. De fleste private brukere etablerer en sesjon hver gang de skal på Internett. Dette vil kunne innebære at samme IP-adresse vil benyttes av forskjellige abonnenter over et tidsrom, men ved fast bredbåndsforbindelse er skifte i IP-adresse som oftest knyttet til brudd på strømlinjen eller tilsvarende svikt i nettforbindelsen.

På Internett finnes databaser som gir en viss oversikt over hvem som disponerer faste IP-adresser (whois). En slik database kan sammenlignes med en telefonkatalog. For å identifisere brukeren av en dynamisk IP-adresse, må man derimot vite hvem som benyttet IP-adressen på et gitt tidspunkt. Slike opplysninger finnes ikke i allment tilgjengelige registre, og en må derfor henvende seg til den aktuelle tilbyder som må sammenholde IP-loggen som opprettes ved internettoppkoblinger med sitt kunderegister. Ved hjelp av loggene kan IP-adressen på et gitt tidspunkt kobles til en bestemt abonnent. Dette innebærer at man er avhengig av at tilbyder faktisk har logget bruken av IP-adressene og oppbevart logginformasjonen.

I dag er det ingen lagringsplikt for logger som opprettes ved internettilkoblinger. Enkelte tilbydere fører ingen slik logg, mens andre lagrer slike

opplysninger av fakturerings- eller sikkerhetshensyn. Ekomloven § 2-7 oppstiller en sletteplikt for data som ikke er nødvendig for kommunikasjons- eller faktureringsformål eller når brukeren ikke selv har samtykket i videre lagring. En lignende sletteplikt følger også av personopplysningsloven § 28 første ledd. I brev 13. mai 2009 fra Datatilsynet til IKT-Norge, orienterte Datatilsynet om følgende vedtak:

> «Personopplysningslovens § 28 setter forbud mot lagring av unødvendige opplysninger. Hovedregelen er at personopplysninger skal slettes når formålet med behandlingen er oppfylt, med mindre det kan påberopes nytt behandlingsgrunnlag.
>
> […]
>
> *Prinsipp bak Datatilsynets retningslinje*
>
> Følgende tolkning legges til grunn:
> 1. Lagring av informasjon om hvilken abonnent som er tildelt en IP-adresse er tillatt for å ivareta driftsrealterte formål. Lagringstiden skal likevel ikke overstige tre uker.
> 2. Leverandøren må basere egen slettepraksis på en konkret vurdering. Kortere slettefrist kan dermed være relevant.»

I høringsnotatet ble det foreslått å videreføre unntaket fra taushetsplikten slik at utlevering til andre myndigheter kan skje der dette er særskilt hjemlet i lov. Hvorvidt denne adgangen bør opprettholdes beror i stor grad på hvilke implikasjoner dette har for personvernet. Abonnements/brukerdata utleveres for å identifisere hvem som innehar et telefon- eller internettabonnement. Behovet for en logg som kobler IP-adresser og abonnementsinformasjon gjelder med dynamiske IP-adresser. Ved statiske IP-adresser følger koblingen mellom abonnent og IP-adresse direkte av offentlig tilgjengelige abonnementsregistre. Loggføringen innebærer slik sett ikke mer enn at bruker av abonnementet er like sporbar som den hadde vært ved en statisk adresse. Tilbyderne leverer ikke ut IP-logger, men utelukkende informasjon om hvem som disponerte en bestemt IP-adresse på et gitt tidspunkt. Dersom kontrollorganet ikke har en konkret IP-adresse og et eksakt oppkoplingstidspunkt er opplysningene omfattet av taushetsplikt. I motsetning til hva som er tilfellet for trafikk- og lokaliseringsdata, vil ikke utlevering av abonnements/brukerdata muliggjøre en nærmere analyse av en persons bevegelses-, atferds- og kommunikasjonsmønster. Dette innebærer at utlevering av abonnements/brukerdata er mindre inngripende enn utlevering av trafikk- og lokaliseringsdata.

Det er et viktig personvernprinsipp at personer skal ha oversikt over hvor opplysninger om en selv befinner seg. Den som tegner et abonnement på hemmelig telefonnummer eller opererer med en dynamisk IP-adresse vil i utgangspunktet ha forventninger om at en svært snever personkrets vil ha kjennskap til hans brukerdata. For å ivareta dette personvernhensynet bør adgangen til utlevering av slik informasjon være snever. Nettopp personvernhensyn er bakgrunnen for at slike opplysninger i dag er taushetsbelagt etter ekomloven § 2-9.

Spørsmålet blir da om nytteverdien av opplysningene tilsier at slik utlevering likevel bør skje. De myndigheter som i dag har hjemmel til å kreve utlevert abonnements/brukerdata er toll-, avgifts- og skattemyndighetene samt Finanstilsynet, jf. henholdsvis tolloven § 12-4 første ledd, merverdiavgiftsloven § 16-3, ligningsloven § 6-13a og verdipapirhandelloven § 15-3 annet ledd nr. 2. Mens de tre førstnevnte kontrollorganer har adgang til å få utlevert opplysninger om navn og adresse til en abonnent som ikke har offentlig telefonnummer eller telefaksnummer, har Finanstilsynet adgang til å innhente alle former for abonnement/brukerdata omfattet av ekomloven § 2-9 tredje ledd.

Hensynet til en effektiv kontroll tilsier at kontrollmyndighetene gis en viss adgang til å innhente abonnent-/brukerdata når det foreligger mistanke om for eksempel brudd på skatte-, avgifts- og tollovgivningen. Det er etter departementets syn viktig at håndhevelsesmidlene ikke går lenger enn behovet tilsier, og at reglene ivaretar hensynet til rettssikkerhet og personvern. Toll-, skatte- og avgiftssystemet er basert på selvdeklarering fra personer og bedrifter. Systemet er basert på tillit, og myndighetenes kontrollarbeid går i stor grad ut på å etterse at opplysningsplikten er oppfylt. For at kontrollarbeidet skal være effektivt, må myndighetene ha tilgang til opplysninger som er nødvendige for å kontrollere at de opplysningspliktige følger regelverket. Når hemmelig nummer benyttes i forbindelse med skatte- og avgiftspliktig aktivitet eller ulovlig inn- og utførsel av varer, tilsier hensynet til effektiv kontroll at kontrollmyndighetene skal ha rett til å få opplyst hvem som står bak.

De ovennevnte lovbestemmelser stiller som vilkår at det foreligger mistanke om overtredelse av bestemmelser gitt i eller i medhold av henholdsvis ligningsloven, merverdiavgiftsloven og tolloven og at særlige hensyn gjør slik utlevering nødvendig. Hvorvidt utlevering skal skje beror således på en

konkret vurdering i det enkelte tilfellet. Forholdet til EMK artikkel 8 ble uttrykkelig vurdert ved innføringen av utleveringshjemlene, og utleveringsadgangen ble funnet å tilfredsstille kravene i artikkel 8 annet ledd, jf. Ot.prp. nr. 21 (1999-2000) Endringer i skatteloven mv. s. 36. Departementet slutter seg til de vurderinger som der ble foretatt. De hjemler for utlevering av identifikasjonsdata som finnes i ligningsloven, merverdiavgiftsloven og tolloven, har blitt utformet med sikte på å sikre en forsvarlig balanse mellom hensynet til vern av privatlivet og hensynet til å avdekke og straffeforfølge lovbrudd. Det er departementets syn at denne vurderingen ikke endres ved at lagringen nå blir obligatorisk ved gjennomføringen av datalagringsdirektivet. Slik departementet ser det, vil kontrollmyndighetene fremdeles ha et behov for å innhente identifikasjonsopplysninger til en abonnent som ikke har offentlig telefonnummer eller telefaksnummer. Kravet om mistanke om lovovertredelser samt at særlige hensyn må gjøre utlevering av opplysningene nødvendig, sikrer at slik innhenting ikke skjer rutinemessig. Avveiningen av kontrollmyndighetenes behov og personverninngrepet tilsier etter departementets syn at den utleveringsadgang som er hjemlet i tolloven § 12-4 første ledd, merverdiavgiftsloven § 16-3 og ligningsloven § 6-13 a bør videreføres.

Også andre offentlige kontrollmyndigheter som har en mer generell lovhjemmel til å innhente opplysninger uavhengig av taushetsplikt, vil kunne få adgang til slike identifikasjonsopplysninger som er omfattet av ekomloven § 2-9 tredje ledd første punktum. Departementet foreslår en endring av ekomloven § 2-9 tredje ledd som klargjør at eventuell hjemmel i lov for andre kontrollmyndigheter til å innhente opplysninger uavhengig av taushetsplikten etter ekomloven, avgrenses til abonnement/brukerdata som nevnt i § 2-9 tredje ledd første punktum.

For alle andre data omfattet av taushetsplikten forutsettes at det foreligger lovhjemmel som fastsetter at taushetsplikten etter § 2-9 ikke skal gjelde og at denne lovhjemmelen er inntatt i opplistingen i femte ledd. Opplistingen i femte ledd er uttømmende. Det betyr at det kun er politi og påtalemyndighet samt Finanstilsynet skal ha adgang til å innhente trafikkdata.

Det har vært en diskusjon om det etter folketrygdloven § 21-4 a i forbindelse med mistanke om trygdemisbruk, kan bes om utlevering av blant annet trafikkdata. Arbeids- og velferdsdirektoratet, Helsedirektoratet eller særskilt utpekte enheter vil i så fall kunne benytte denne hjemmelen. Departementet går inn for at det foruten utlevering til politi og påtalemyndighet, bare skal være adgang til å utlevere trafikkdata til Finanstilsynet, jf. nærmere redegjørelse under kapittel 14.5.2 om bakgrunnen for dette. Det er således på det rene at NAV ikke skal ha adgang til å innhente trafikkdata.

14.5.2 Særlig om Finanstilsynets tilgang

Finanstilsynets utleveringshjemmel i verdipapirhandelloven § 15-3 annet ledd nr. 3 bygger på EU-direktiver som Norge er forpliktet til å gjennomføre i nasjonal rett. Dette ble også lagt til grunn i verdipapirhandellovens forarbeider, jf. Ot.prp. nr. 34 (2006-2007) Om lov om verdipapirhandel (verdipapirhandelloven) og lov om regulerte markeder (børsloven) s. 259. Bestemmelsen gjennomfører direktiv 2003/6/EF om markedsmisbruk (markedsmisbruksdirektivet) og direktiv 2004/39/EF om markeder for finansielle instrumenter (MiFID). Av hensyn til behovet for å bekjempe kriminalitet og samtidig beholde et sterkt personvern for den enkelte, mener departementet at utlevering av data bare skal skje til politi og påtalemyndighet. Fra dette standpunktet må det imidlertid gjøres et unntak av hensyn til våre folkerettslige forpliktelser for så vidt gjelder Finanstilsynet.

Markedsmisbruksdirektivet ble vedtatt 28. januar 2003, og ble gjennomført i norsk rett ved endringer i verdipapirhandelloven av 1997 med ikrafttredelse 1. september 2005. Hovedformålet med direktivet er å sikre integriteten til verdipapirmarkedene i EØS-området, herunder forbedre investorenes tillit til disse markedene. Direktivet har utførlige regler om tilsyn med markedsmisbruksregelverket som skal sikre en homogen og effektiv håndhevelse. Det er lagt opp til at tilsynskompetansen skal samles hos ett organ i hver medlemsstat, kalt «the competent authority», jf. artikkel 1 nr. 7, jf. artikkel 11. Tilsynsorganets kompetanse er nærmere regulert i direktivet artikkel 12. I henhold til artikkel 12 nr. 2 skal tilsynsorganet ha visse minimumsbeføyelser, blant annet tilgang til eksisterende trafikkdata («existing telephone and existing data traffic records«), jf. art. 12 nr. 2 bokstav d. I Ot.prp. nr. 12 (2004-2005) Om lov om endringer i verdipapirhandelloven og enkelte andre lover (gjennomføring av markedsmisbruksdirektivet) la departementet til grunn at Finanstilsynet bør ha kompetanse til å innhente trafikkdata sett hen til EØS-forpliktelsenes omfang (s. 108). Kravet i markedsmisbruksdirektivet art. 12 nr. 2 bokstav d, sammen med behovet for snarlig tilgang til datatrafikk for effektiv bekjempelse av ver-

dipapirkriminalitet var også bakgrunnen for lovendringen i verdipapirhandelloven av 1997 § 12-2a som på visse vilkår ga Finanstilsynet tilgang til trafikkdata ved mistanke om brudd på bestemmelser som gjennomfører direktivet.

MiFID ble vedtatt 21. april 2004 og gjennomført i norsk rett ved vedtakelsen av ny verdipapirhandellov av 2007. Hovedformålet med direktivet er å bidra til å utvikle og sikre de europeiske verdipapirmarkedenes effektivitet, integritet, samt oversiktlighet og tillit til markedet. Direktivet inneholder blant annet regler om verdipapirforetaks og regulerte markeders (dvs. børser og autoriserte markedsplassers) organisering og virksomhet samt bestemmelser om tilsyn med verdipapirforetak og regulerte markeders virksomhet og overholdelse av lovgivning. Mens markedsmisbruksregelverket retter seg mot enhver, er det altså verdipapirforetak og regulerte markedene som er pliktsubjekter etter MiFID. MiFID inneholder på lik linje med markedsmisbruksdirektivet en liste over tilsynsmyndighetenes minimumsbeføyelser, herunder et krav om at Finanstilsynet som «competent authority» skal ha tilgang til trafikkdata («existing telephone records and existing data traffic») for å føre tilsyn med at direktivbestemmelsene overholdes, jf. direktivet art. 50 nr. 2 bokstav d. Forpliktelsen ble gjennomført ved verdipapirhandelloven § 15-3 annet ledd nr. 2, som hjemlet tilsynets innhenting av trafikkdata. Bestemmelsen er i det vesentlige en videreføring av verdipapirhandelloven 1997 § 12-2a, likevel slik at utleveringsadgangen ble utvidet til å gjelde mistanke om verdipapirforetaks overtredelse som gjennomfører MiFID.

Så vel markedsmisbruksdirektivet som MiFID åpner for at tilsynsorganets kompetanse til å innhente trafikkdata kan være betinget av samarbeid med andre myndigheter, jf. markedsmisbruksdirektivet artikkel 12 nr. 1 bokstav b og MiFID artikkel 50 nr. 1 bokstav b. En kunne således tenke seg en ordning hvoretter Finanstilsynet, ved mistanke om lovbrudd, måtte henvende seg til politiet, som så kunne begjære trafikkdata utlevert på vegne av tilsynet.

Både markedsmisbruksdirektivet og MiFID legger i stor grad opp til at tilsynsmyndighetene selv skal forfølge og irettefø̈re brudd på direktivbestemmelsene, herunder iverksette administrative sanksjoner, jf. markedsmisbruksdirektivet art. 14 og MiFID art. 51. Finanstilsynets innhenting skjer ikke som ledd i en straffesak, men er et tiltak dette forvaltningsorganet foretar som ledd i sin kontroll med at lovgivningen på verdipapirområdet blir overholdt.

Der Finanstilsynet på et tidlig stadium i undersøkelsene må henvende seg til politiet for å be om tilgang til trafikkdata, vil saken, ut fra dagens arbeidsfordeling mellom politiet og Finanstilsynet, etter tilsynets erfaring fortsette i et strafferettslig spor. Administrative sanksjoner vil da i praksis ikke bli aktuelle. Hensynet til en effektiv tilsyns- og sanksjonskompetanse for Finanstilsynet tilsier at tilsynet selv bør kunne innhente trafikkdata.

Etter departementets syn er det kravet om rettens kjennelse som er den sentrale garantien for at hensynet til personvern og rettssikkerhet blir tilstrekkelig ivaretatt. Kravet om rettens kjennelse er nytt i forhold til gjeldende rett. I dag treffer Finanstilsynet vedtaket som pålegger tilbyderne å utlevere trafikkdata, riktignok forutsatt at Post- og teletilsynet gir tilbyderne et slikt fritak fra taushetsplikten i ekomloven § 2-9. En ser ikke umiddelbart at en ordning hvor politiet innhenter trafikkdata på vegne av tilsynet, bidrar til ytterligere styrking av personvernet. Departementet mener derfor at Finanstilsynets tilgang til data som bygger på markedsmisbruksdirektivet og MiFID, best kan gjennomføres i norsk rett ved at tilsynet gis direkte adgang til å kreve utlevering av trafikkdata.

Et særlig spørsmål er om det bør gjelde et særlig strafferammekrav for utlevering av trafikkdata til Finanstilsynet, slik departementet foreslår for utlevering til politiet og påtalemyndigheten. Grunnvilkåret for Finanstilsynets begjæring er i dag at det foreligger konkret mistanke om overtredelse av verdipapirhandelloven kapittel 3, 4, 5, 8, 9, 10 eller 11, eller forskrifter gitt i medhold av disse bestemmelsene, jf verdipapirhandelloven § 15-3 annet ledd nr. 3. Det er her tale om lovbrudd med ulik alvorlighetsgrad, og følgelig ulik strafferamme. Selv om departementets klare utgangspunkt er at Finanstilsynets tilgang til trafikkdata ikke bør være videre enn det som gjelder for politi- og påtalemyndighet, antar en at innføring av særlige strafferammekrav vil bryte med forpliktelsene etter markedsmisbruksdirektivet og MiFID.

Innhenting av trafikkdata kan utgjøre et alvorlig inngrep i privatlivet til den det gjelder, og departementet går inn for at hjemmelen ikke skal omfatte flere typer data enn våre folkerettslige forpliktelser tilsier. I forlengelsen av dette vil departementet presisere at Finanstilsynets tilgang til data bare gjelder abonnements-/brukerdata, jf. ekomloven § 2-9 sammenholdt med verdipapirhandelloven § 15-3 annet ledd nr. 2, og trafikkdata. Innføring av lagringsplikt vil medføre lagring av

flere data enn i dag og dermed gi Finanstilsynet økt tilfang til data. Lokaliseringsdata er særlig inngripende for personvernet og faller også utenfor de forpliktelser som ligger til grunn for verdipapirhandelloven § 15-3 annet ledd nr. 3.

Utleveringsbestemmelsen i straffeprosessloven § 210 åpner for hastekompetanse for politi og påtalemyndighet. Departementet kan ikke se at det følger av verken markedsmisbruksdirektivet eller MiFID at Finanstilsynet skal ha en slik adgang.

14.5.3 Om bruk av trafikkdata som bevis i sivile saker

Departementet legger til grunn at de begrensninger i adgangen til trafikkdata og lokaliseringsdata som skal gjelde for andre myndigheter enn Finanstilsynet, jf. ovenfor for så vidt gjelder trafikkdata, også bør gjelde i sivile saker. Det innebærer at tvisteloven § 22-3 bør endres slik at den taushetsplikt som gjelder for tilbyderne i medhold av ekomloven § 2-9 for så vidt gjelder trafikkdata og lokaliseringsdata, skal gjelde uten mulighet for at Post- og teletilsynet eller eventuelt retten kan oppheve denne. Dette er i tråd med prinsippet om at dataene lagres for kriminalitetsbekjempende formål.

Samtidig bør dagens adgang til å få utlevert abonnementsopplysninger, herunder også elektronisk kommunikasjonsadresse, beholdes jf. kapittel 14.2.2. Dette er mer alminnelige opplysninger som likevel kan ha stor betydning i private saker, typisk for å avsløre hvem som står bak immaterialrettskrenkelser, jf. ovennevnte kjennelse fra Høyesterett i den såkalte Altibox-saken. Her slo domstolen fast at retten med hjemmel i tvisteloven kapittel 28 sammenholdt med tvisteloven § 22-3, kan tillate at visse opplysninger underlagt lovbestemt taushetsplikt etter ekomloven, sikres som bevis utenfor rettssak. Slike data er underlagt et mindre strengt vern, jf. Høyesteretts syn om at «denne type opplysninger ved strafferettslig etterforskning har et svakere vern enn for eksempel trafikkdata» (dommen avsnitt 41). I begrunnelsen slutter Høyesterett seg videre til lagmannsrettens lovforståelse om at private bør få tilgang til slike opplysninger for å ha mulighet til å fremme erstatningssøksmål uavhengig av sakens strafferettslige side (i avsnitt 52):

> «Lagmannsrettens flertall har også som et vesentlig moment, vist til at Internett på mange måter fungerer tilnærmet på linje med ordinær telefonbruk, og at dette tilsier at brukerne forventer at deres bruk er skjermet for offentlig innsyn. Flertallet mente videre at den omstendighet at ankemotpartene ikke har meldt forholdet til politiet ikke kan tillegges vekt når siktemålet med begjæringen er å fremskaffe grunnlag for et erstatningskrav for krenkelsene av deres rettigheter. Flertallet oppsummerer sitt syn slik:
>
> 'Etter en samlet vurdering – blant annet særlig hensyntatt at det dreier seg om en handling som antas å være både straffbar og erstatningsbetingende, politiets manglende prioritering av slike saker, den omstendighet at abonnenten av den aktuelle IP-adressen ikke kan ha en berettiget forventning om rettsstridig bruk av denne og de motstridende hensyn som er nevnt over – kan ikke flertallet se at det vil være uforholdsmessig å gi Sandrew m.fl. tilgang til identiteten til abonnenten av den aktuelle IP-adressen.'»

Departementet foreslår ikke endringer i tvisteloven § 22-3 annet ledd. Dette innebærer at Post- og teletilsynets fritak fra taushetsplikten som utgangspunkt fortsatt er et vilkår for at retten kan tillate at abonnements- eller brukerdata føres som bevis under sivile søksmål.

15 Tilsyn

15.1 Gjeldende rett

I henhold til artikkel 9 i EUs datalagringsdirektiv skal medlemslandene gi en eller flere offentlige myndigheter ansvaret for å føre tilsyn med datasikkerheten hos tilbyder. I dag er ansvaret for å føre tilsyn med informasjonssikkerheten og behandling av personopplysninger hos ekomtilbydere etablert i Norge, delt mellom Post- og teletilsynet og Datatilsynet. Post- og teletilsynet fører tilsyn med hjemmel i lov om elektronisk kommunikasjon 7. april 2003 nr. 83 kapittel 10, mens det rettslige grunnlaget for Datatilsynets tilsyn er lov om behandling av personopplysninger 14. april 2000 nr. 31 §§ 42 og 44.

Post- og teletilsynet har et generelt tilsynsansvar etter ekomloven for å sikre at krav fastsatt i eller i medhold av loven oppfylles, jf. § 10-1. 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.

Post- og teletilsynet er videre tilsynsmyndighet når det gjelder tilbyders tilretteleggingsplikt etter ekomloven § 2-8 om tilrettelegging for lovbestemt tilgang til informasjon. I tillegg har Post- og teletilsynet et særlig personvernrelatert tilsynsansvar som knyttes opp mot bestemmelsene om tilbyders taushetsplikt i ekomloven § 2-9.

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 personopplysninger som er nedfelt i eller i medhold av loven følges. Etter personopplysningsloven §§ 46 og 47 har Datatilsynet kompetanse til å ilegge overtredelsesgebyr eller tvangsmulkt dersom behandlingsansvarlig ikke overholder gjeldende personopplysningsregelverk.

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. personopplysningsforskriften § 7-1 og Datatilsynets konsesjoner.

Datatilsynets tilsynsansvar 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 dette området. Departementet viser til at det foreligger en avtale mellom Post- og teletilsynet og Datatilsynet om utøvelse av tilsyn.

15.2 Høringsnotatets forslag

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. I høringsforslaget la departementene opp til at Post- og teletilsynet også fremover skal føre tilsyn med at tilbyder faktisk lagrer relevante data etter den foreslåtte bestemmelsen om lagringsplikt. Videre ble det foreslått 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 for kriminalitetsbekjempelsesformål.

Ekomloven § 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 inn for avgjørelse hos myndigheten. Dette betyr at kompetente myndigheter med lovbestemt tilgang til data som det i medhold av loven påhviler tilbyder å lagre, kan bringe spørsmålet inn 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. I høringsnotatet ble det ikke foreslått endringer i tilsynsoppgavene til Post- og teletilsynet.

Departementene gikk i høringsnotatet inn for å videreføre Datatilsynets tilsynsansvar etter personopplysningsloven også for data som lagres i medhold av den foreslåtte bestemmelsen om lagringsplikt. Høringsforslaget la ikke opp til at Datatilsynet skal tillegges særskilt tilsynskompetanse etter ekomloven.

Departementene viste i høringsnotatet til at det foreligger en avtale mellom Post- og teletilsynet og Datatilsynet for utøvelse av delt tilsyn. Departementene forutsatte at denne avtalen videreføres og oppdateres i forbindelse med innføring av en ny lagringsplikt.

15.3 Høringsinstansenes syn

Arbeidsdepartementet, Politijuristene, GET, NetGenTel, Nord-Trøndelag politidistrikt, IKT-Norge, ITAKT, Post- og teletilsynet, Akademikerne, TEKNA og *NorSIS* har uttalt seg om tilsynsspørsmålet. De fleste av disse, er av den oppfatning at videreføring av dagens delte tilsynsansvar er uproblematisk. *Arbeidsdepartementet* påpeker likevel at et velfungerende og aktivt tilsyn er viktig for at borgerne skal oppleve at personvernet blir ivaretatt. *GET* og *NextGenTel* er opptatt av at både tilbydere og kunder må kunne vite hvilket tilsynsorgan som har ansvaret for hva. Også *Nord-Trøndelag politidistrikt* viser til at det er viktig at etatene avklarer området for sin tilsynskompetanse, slik at det er klart definerte ansvarsområder. *Post- og teletilsynet* selv har heller ingen innvendinger mot felles tilsyn med Datatilsynet, men påpeker at det krever styrket samordning av tilsynsarbeidet.

Nord-Trøndelag politidistrikt uttaler:

> «Forslaget om å videreføre det delte tilsynsansvaret mellom Post- og teletilsynet og Datatilsynet:
>
> Under dette punktet støtter politidistriktet forslaget om at delingen mellom Post- og teletilsynet og Datatilsynet videreføres. Det er viktig at etatene avklarer områdene for sin tilsynskompetanse slik at man har klart definerte ansvarsområder».

Post- og teletilsynet uttaler:

> «Departementene foreslår et tilnærmet likt tilsynsansvar som i dag og at PT fortsatt skal dele tilsynsansvaret med Datatilsynet. PT støtter departementenes forslag vedrørende tilsyn. I den forbindelse ser PT at det vil være behov for å styrke samarbeidet med Datatilsynet og at eventuelle stedlige tilsyn må samordnes».

NorSIS er imidlertid skeptisk til delt tilsynsansvar, da de mener det vil være uklart hvem som har ansvar for hva, og savner også en nærmere redegjørelse for tilsynsutfordringer andre land har møtt på.

NorSIS uttaler:

> «NorSIS stiller spørsmål ved om en deling av tilsynet, kan medføre at noe kan falle mellom to stoler. F.eks. hvem fører tilsyn med at direktivets formål, nødvendighet og proporsjonalitet, bruk av overskuddsinformasjon blir overholdt».

Politijuristene påpeker at Datatilsynet kan være inhabile som tilsynsorgan pga. sin motstand mot datalagringsdirektivet.

Politijuristene uttaler:

> «En sak som fortjener en særskilt kommentar er Datatilsynets rolle som tilsynsorgan. Problemstillingen er ikke nevnt i høringsnotatet, men vi finner likevel grunn til å kommentere det. For det tilfellet at datalagring innføres, vil lagringen kontrolleres av både Datatilsynet og Post og teletilsynet. Dette framgår av høringsnotatets pkt. 4.10, særlig pkt. 4.10.2. Dette er en konsekvens av at Datatilsynet er kontrollorgan etter personopplysningsloven, mens PT er det etter lov om elektronisk kommunikasjon. Datatilsynet har etter personopplysningsloven § 42 en rolle som uavhengig forvaltningsorgan med to ulike funksjoner: dels et tilsynsorgan og dels et fristilt organ som skal delta i samfunnsdebatten. Datatilsynet er motstander av direktivet. I tilsynets bemerkninger beskrives datalagring som «totalitært svermeri». Dette uttrykket har tilsynet brukt gjentatte ganger i flere år for å beskrive datalagring.
>
> Dette skaper spørsmål som kan nærme seg inhabilitet. Skal Datatilsynet føre tilsyn med et tiltak som tilsynet ikke ønsker innført? Datatilsynet er ikke en stor virksomhet, med knapt 40 ansatte på ett felles arbeidssted. Dette gjør det vanskelig å ha «kinesiske vegger», som skiller

personer som gjør ulike oppgaver. Tilsynet har heller ikke noe styre eller andre som fører tilsyn med den daglige driften. En kan kanskje også si at det ikke er fair overfor Datatilsynet at de – som en konsekvens av lovens system – i tilfelle må føre tilsyn med en virksomhet som tilsynet offentlig har tatt avstand fra».

Akademikerne, TEKNA og *ITAKT* tar til ordet for opprettelse av et uavhengig kontrollorgan for jevnlig kontroll av bruk av trafikkdata som supplement til tilsynsorganene.

TEKNA uttaler:

«Datatilsynet og Post- og teletilsynet overlapper hverandre noe innenfor dette område. Begge vil være sentrale og få betydelig oppgaver hvis DLD innføres. Vi forutsetter derfor at det settes av tilstrekkelig med ressurser, slik at disse tilsynsmyndighetene kan ivareta nye, krevende oppgaver på en god måte.

Spørsmålet er imidlertid om dette er tilstrekkelig innenfor et så viktig område. Hvis det åpnes for lagring som DLD gir mulighet til, burde man i tillegg til de nevnte tilsyn vurdere periodevise gjennomganger av rammen og bruken av data. Kommisjoner eller ombud som ikke er forankret i de utøvende myndigheter kan være egnet til dette. På samme måte som det er ombud for forvaltningen, utpekt av Stortinget, burde det være et ombud eller en kommisjon, tilsvarende Lund-kommisjonen, som har som oppgave å vurdere hvordan myndighetene utøver kontroll med lagring av data og får tilgang til data. En slik kommisjon eller ombud kunne ha som oppgave å foreta regelmessige gjennomganger, og presentere disse for Stortinget for eksempel hvert fjerde år. For øvrig vil den som føler seg krenket ved myndighetenes bruk av lagrede data kunne bringe saken inn for norske domstoler og internasjonale organer for menneskerettigheter».

15.4 Departementets vurdering

Departementet registrerer merknaden fra *Politijuristene* om at Datatilsynet kan være inhabil som tilsynsmyndighet på grunn av sin motstand mot datalagringsdirektivet. Til dette vil departementet bemerke at Datatilsynet allerede i dag fører tilsyn med flere behandlinger av personopplysninger som tilsynet har uttalt seg kritisk om. Dette gjelder for eksempel en del personregistre i helsesektoren, og det gjelder behandling av personopplysninger i samferdselssektoren. Dette har ikke tidligere vært anført som problematisk, og departementet er heller ikke kjent med at det har representert noe problem for gjennomføringen av tilsynsarbeidet. Dessuten bemerkes det at Datatilsynet ikke skal føre tilsyn med *om* det lagres data, men at de data som lagres, faktisk lagres på forsvarlig vis.

NorSIS bemerker at det kan være problematisk å vite hvilket tilsyn som har ansvar for hva. Departementet viser til at det i hovedsak vil være snakk om å videreføre gjeldende rett, og at de utfordringene *NorSIS* peker på ikke har skapt store problemer til nå. Dette er uansett temaer som vil være gjenstand for regulering i samarbeidsavtalen mellom Datatilsynet og Post- og teletilsynet. *NorSIS* savner videre en redegjørelse for tilsynsutfordringer i andre land. Etter det departementet kjenner til, har spørsmålet om delt tilsyn ikke vært tema i noen av de rapporter som er utarbeidet om implementering av datalagringsdirektivet i EU. Trolig er dette en konsekvens av at delt tilsynsansvar ikke har representert noe nevneverdig problem i de statene der delt tilsynsansvaret forekommer.

Når det gjelder forslaget fra enkelte høringsinstanser om å opprette et eget kontrollorgan for kontroll med politiets bruk av data, viser departementet til at rettsikkerheten knyttet til utlevering av data nå er foreslått betydelig styrket. Det vises til innføring av domstolskontroll med utlevering, samt betydelig skjerpelse av vilkårene for utlevering. I forbindelse med domstolsbehandlingen skal den som rammes av beslaget underrettes. På denne bakgrunn kan en ikke se at det er nødvendig å etablere et kontrollutvalg for data (jf. KK-utvalget).

Allerede i dag deler Datatilsynet og Post- og teletilsynet tilsynsansvar på ekom-området, uten at dette er påpekt som problematisk fra noe hold. Datatilsynet deler også tilsynsansvar med andre myndigheter, blant annet Helsetilsynet, uten at dette fremstår som problematisk. Departementet er enig med de høringsinstansene som mener at fortsatt delt tilsynsansvar på ekom-området er uproblematisk. Det foreslås derfor at dagens tilsynsordning, med et delt tilsynsansvar mellom Post- og teletilsynet og Datatilsynet, videreføres. Det er imidlertid viktig at både tilsynsorganene selv, ekomtilbyderne og publikum vet hvilket organ som fører tilsyn med hvilket regelverk, og hvor man kan henvende seg om ulike spørsmål relatert til datalagring. Departementet vil derfor følge opp arbeidet med en styrking av den samarbeidsavtalen som allerede foreligger mellom de to tilsynene.

15.5 Nærmere om lovforslaget

Det foreslås ikke endringer i gjeldende regelverk om Post- og teletilsynets og Datatilsynets delte tilsynsansvar. Det vises imidlertid til at de foreslåtte endringer av bestemmelsene i ekomloven innebærer nye tilsynsoppgaver for Post- og teletilsynet. Blant annet vil innføring av lagringsplikten som foreslås tatt inn i ekomloven § 2-7a innebære en plikt for Post- og teletilsynet til å føre tilsyn med at lagringen skjer. Videre vil det være tilsynsoppgaver knyttet til eventuelle kvalitetskrav eller tekniske standarder som fastsettes i forskrift, ved enkeltvedtak eller i medhold av avtaler med tilbyderne, jf. forslag til § 2-7a, annet ledd. Også krav til tiltak som skal etablere nødvendig sikkerhet i tilbyders systemer mot uhjemlet tilgang til lagrede data, vil måtte følges opp med tilsyn.

15.5.1 Statistikk

Det fremgår av datalagringsdirektivets artikkel 10 at medlemslandene er forpliktet til årlig å sende inn statistikk til EU-kommisjonen om datalagringen. Ved en innføring av datalagringsdirektivet i norsk lov forplikter norske myndigheter seg tilsvarende å sørge for årlig statistikk til ESA om datalagring. I høringsnotatet foreslo departementene at politiet og andre myndigheter som anmoder om data skal føre denne statistikken og videresende den til Post- og teletilsynet for oversendelse til ESA. Begrunnelsen for at Post- og teletilsynet skal gjøre dette er at implementeringen av direktivet vil være med referanse til vedlegg 11 om telekommunikasjon i EØS-avtalen. Ingen høringsinstanser med unntak av Post- og teletilsynet har særlige merknader til dette forslaget. Post- og teletilsynet er enig i at de bør inneha rollen som oversender til ESA. Dette vil kunne gi tilsynet innsyn i hvordan tilbyderne oppfyller sin forpliktelse i henhold til ekomloven. Tilsynet legger imidlertid til grunn at deres ansvar ikke vil omfatte koordinering og innhentingen av data fra alle politidistrikt og særorgan.

Departementet opprettholder forslaget fra høringsnotatet om at politiet og andre myndigheter, som i henhold til lovforslaget kun er Finanstilsynet, skal føre statistikk over følgende:

- antall saker hvor anmodninger blir imøtekommet
- tiden mellom lagringstidspunkt (dato) og etterspørsel etter data
- antall saker der anmodning om data ikke har blitt imøtekommet

Samlet statistikk fra henholdsvis politiet og Finanstilsynet skal årlig oversendes Post- og teletilsynet, som skal videreformidle denne til ESA. Det vil være opp til ESA å beslutte om Norge skal benytte samme skjema for rapportering som medlemslandene i EU benytter.

16 Økonomiske og administrative konsekvenser

Datalagringsdirektivet regulerer ikke kostnadsspørsmålet. Departementet 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. Medlemslandene har valgt ulike modeller for kostnadsdeling. I noen land får tilbyderne dekket alle kostnader knyttet til lagring og uthenting, mens i andre land må tilbyderne selv dekke alle kostnadene. I Danmark må tilbyderne dekke merkostnadene som følge av lagringsplikten, mens politiet betaler for uthenting. I Finland vil alle merkostnadene bli dekket av justismyndighetene.

16.1 Gjeldende rett

Dagens kostnadsmodell i Norge når det gjelder lovbestemt tilgang til informasjon, er en delingsmodell hvor ekomtilbyderne skal tilrettelegge nett og tjenester for lovbestemt tilgang til informasjon om sluttbruker, og forutsettes å dekke kostnadene knyttet til denne plikten. Tilbydernes driftskostnader knyttet til oppfyllelse av tilretteleggingsplikten dekkes av staten. Gjeldende praksis er at politiet betaler for uthenting av informasjon i henhold til avtaler jf. ekomloven § 2-8, andre ledd.

16.2 Høringsnotatets forslag

Departementene foreslo i høringsnotatet ikke noen endring av dagens kostnadsmodell. Kostnadsbildet vil ved innføring av direktivet kunne bli noe annerledes enn i dag, men det er utfordrende å skulle si noe eksakt om kostnadene, all den tid de ulike tilbyderne har ulike tekniske løsninger og tilbyr ulike tjenester. 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 tre økonomiske utredninger av konsekvensene knyttet til innføring av en lagringsplikt.

16.3 Økonomiske utredninger og analyser

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

Utredningen var begrenset til lagring av data knyttet til fasttelefoni, mobiltelefoni og visse aspekter ved internettaksess. Den viste at lagringstid og lagringsvolum i liten grad påvirker kostnadene. Kostnadsfordelingen mellom tilbyder og myndigheter varierer relativt lite ved ulik lagringstid og lagringsvolum. Utviklingstid er den faktoren som i størst grad påvirker kostnadene. Informasjonssikkerhet virker til en viss grad inn på kostnadene, men er ikke svært kostnadsdrivende.

Denne utredningen er i dag mindre relevant siden den ikke omfattet alle lagringspliktene etter direktivet, men kun lagring av data knyttet til fasttelefoni, mobiltelefoni og internettilgang. Lagringsplikt knyttet til E-post og IP-telefoni var ikke med i utredningen.

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

Analysen fra 2008 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.

Analysen 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.

Den tredje utredningen fra april 2010 er en utdypning av den foregående utredningen. Denne analysen har som formål å gi noen presiseringer og tydeliggjøring av merkostnadene for tilbydere og myndigheter ved innføring av datalagringsdirektivet. Blant annet ønsket departementene svar på hvorvidt tilbyderne kan bygge videre på de systemene de har for tilrettelegging i dag, eller om de må etablere helt nye lagringssystemer.

Hovedkonklusjonene fra Teleplans utdypning er at med de systemkrav og forutsetninger som ble gitt om tilgang og sikkerhet, vil tilbyderne måtte utvikle og implementere *nye* systemer for lagring. For tilbyderne samlet vil kostnaden for dette være 217 MNOK over en femårsperiode. Man baserer seg da på at de små tilbyderne vil implementere en felles standardisert løsning. Det er liten kostnadsreduksjon som følge av delvis bortfall av dagens ordning for lagring og uthenting. Merkostnader er således i størrelsesordenen tilsvarende de samlede kostnadene.

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

16.4 Høringsinstansenes syn

Finansdepartementet, Kulturdepartementet, Nærings- og handelsdepartementet, Post- og teletilsynet, NAV, Domstolsadministrasjonen, Kripos, Politidirektoratet, Politijuristene, Universitetet i Oslo matematisk-naturvitenskapelige fakultet, Politiets Fellesforbund, Forbrukerrådet, Norges Juristforbund-Privtat, IKT-Norge, Telenor, NetCom, NextGenTel, Kabel Norge, Altibox, NTV, Ventelo, Tele2, TDC, Get, Forsvarergruppen av 1997, NITO, TEKNA, NORSIS, Abelia, NHO, NHO-reiseliv, UNIO og *LO* har merknader til de økonomiske og administrative konsekvensene ved innføring av datalagringsdirektivet.

Finansdepartementet avventer de ytterlige vurderinger om kostnader og forutsetter at økte administrative kostnader vil bli dekket innenfor Datatilsynets rammer og gjennom kostnadsriktig justering av Post- og teletilsynets gebyrer. *Kulturdepartementet* mener at også de indirekte økonomiske konsekvensene for private interesser burde analyseres. *Nærings- og handelsdepartementet* mener det bør vurderes om staten skal dekke alle kostnadene til lagringsplikten fordi denne saken primært dreier seg om å ivareta generelle sam-

funnsinteresser knyttet til kriminalitetsbekjempelse.

Post- og teletilsynet understreker at gjennomføringen ikke må belaste tilbyderne uforholdsmessig. Høye kostnader vil kunne være en etableringshindring for nye aktører i markedet. *Post- og teletilsynet* uttaler:

> «I utgangspunktet støtter PT en videreføring av prinsippene i dagens ordning, hvor kostnader deles mellom tilbydere og politimyndighet. Dersom det imidlertid skulle vise seg at implementering påvirker konkurransen i ekommarkedet, mener PT at man må vurdere å legge en større del av kostnadene på de offentlige myndigheter. Dette fordi innføringen av lagringsplikt utelukkende har som formål å støtte kriminalitetsbekjempelsen, noe som er en samfunnsoppgave.»

Telenor peker på at forutsetningene for å sette opp et regnestykke er både usikre og uklare, og Telenor velger derfor ikke å antyde et tall for estimerte kostnader forbundet med Telenors eventuelle implementering av datalagringskravene. Av samme grunn har Telenor valgt å avstå fra å kommentere på Teleplans økonomiske konsekvensutredninger.

Telenor vil likevel peke på de vesentlige kostnadsdriverne som vil påvirke kostnadene av lagringspliktige ekomtjenester:

> «*Lagringskravets omfang:* Kostnadene ved å legge til rette for innsamling og lagring av data som i dag ikke lagres eller er tilgjengelige vil kunne være omfattende.
>
> *Krav om logisk atskillelse:* Krav om at data som skal lagres i henhold til direktivet må holdes logisk adskilt fra andre data ekomtilbyderne lagrer, innebærer i praksis at det må utvikles et nytt system for datalagringen. Dette betyr at også de tilbyderne som logger data i dag og som har en infrastruktur og et nettverk som støtter lagring av data, likevel vil måtte investere i nye systemer, nye lisenser, nytt utstyr, mer lagringsplass med videre.
>
> *Lagringsperiode:* Kostnadene vil øke desto lenge man skal lagre data, dette på grunn av at datamengden øker. I tillegg vil det påløpe større kostnader og høyere risiko fordi kapasitet og hastighet må økes for å kunne gjennomføre sikkerhetskopiering innen rimelig tid. Kostnadene vil inntil en viss grad øke lineært i forhold til økt lagringstid, men når man kommer til et kritisk høyt nivå i datamengde vil en større investering i kapasitet måtte gjøres. Det samme vil være tilfelle dersom datamengden øker på grunn av økt trafikk, men denne utviklingen vil være mye vanskeligere å forutsi.
>
> *Krav til utlevering:* Dersom man pålegger operatørene korte leveringsfrister vil krav til automatisering og bemanning, og dermed også kostnadene, øke i forhold til systemstøtte.
>
> *Detaljeringsgrad:* Det vil *være svært* kostnadsdrivende for operatørene dersom det blir avkrevd høy detaljeringsgrad i rapporter til myndighetene. Hvis man for eksempel skal hente ut rapporter med navn, adresse mv. pr. avsender og mottaker, vil dette være svært kapasitetskrevende.
>
> *Krav til redundans/reserveløsninger:* Dersom det blir satt høye SLA-krav i forhold til feil- og katastrofesituasjoner vil det være nødvendig å etablere redundante systemer, alternativt reserveløsninger. Dette vil være svært kostnadsdrivende, da alt må dubleres og ekstra teknologi må innføres for å håndtere dette.
>
> *Datakvalitet:* Kvaliteten på data som ikke har vært ansett som nødvendige for fakturering, har ikke nødvendigvis samme kvalitet som faktureringsdata. I og med at slike data normalt benyttes forbindelse med drift, vedlikehold og feilsøking, er behovet for nøyaktighet her ikke det samme som for fakturering. Dette betyr blant annet at man ikke har samme krav til at alt blir logget, eller at tidspunkt er like nøyaktig som i de deler av infrastrukturen som benyttes til eksempelvis taksering. Utbedring av dette kan kreve kostbare endringer av systemer, eller være svært vanskelig å få til i praksis.
>
> Telenor, har begrensede ressurser til rådighet for IS/IT-utvikling og oppfølging av regulatoriske pålegg. Allerede i dag er bransjen underlagt en lang rekke sektorspesifikke krav. Selv om myndighetene bestemmer seg for full statlig finansiering av kostnadene ved implementering av datalagringsdirektivet, vil tilbyderne likevel måtte bruke betydelig både tid og ressurser på å følge opp kravet».

NextGentel mener myndighetene må vurdere tilretteleggingsstøtte. Det vil gi bedre kvalitet på implementeringen. Tilskudd kan i følge NextGentel enten gis direkte eller som skattefradrag. Også *NTV* mener en tilskuddsordning bør vurderes. *Kabel Norge* mener alle kostnader ved datalagringsdirektivet må dekkes av det offentlige, jf. Finland. Kabel Norge mener man ikke automatisk kan videreføre dagens kostnadsmodell. *Ventelo*

mener det ikke er naturlig å videreføre dagens fordelingsmodell. *Ventelo* uttaler:

> «I dag lagres data for kommersielle og/eller driftsmessige forhold. Lagring i henhold til datalagringsdirektivet gjennomføres for å bekjempe kriminalitet. Tilbydernes egne interesser faller i sin helhet utenfor formålet med lagringen, [...]»

NetCom, Altibox, Tele2, TDC og *Get* mener også at myndighetene må dekke kostnadene. *Tele2* uttaler:

> «Departementet foreslår en delingsmodell hvor ekomtilbyderne har en tilretteleggingsplikt, og dekker kostnadene til denne plikten, mens drifts/uthentingskostnader dekkes av politiet i henhold til avtaler. Tele 2 er av den oppfatning at alle kostnader, både tilretteleggingskosten og drifts/uthentingskostnader, må dekkes av politiet. De private databasene som blir opprettet som en følge av datalagringsdirektivet, gjøres på vegne av politiet, og det er naturlig at den som skal benytte informasjonen også betaler for hele systemet som innføringen av datalagringsdirektivet innebærer».

IKT-Norge mener det vil være totalt urimelig dersom noen av kostnadene forbundet med datalagringsdirektivet legges på ekomtilbyderne. *IKT-Norge* sier:

> «Vi anerkjenner ikke at en modell for kostnadsdeling som benyttes i dag ved utlevering av trafikkdata etter ekomlovens § 2-8 andre ledd har noen som helst relevans. Denne bestemmelsen omhandler utlevering av trafikkdata selskapene allerede henter inn til eget bruk for å sikre kvaliteten på de tjenester de leverer sine kunder. Altså har selskapene en egeninteresse av å framskaffe disse data. Datalagringsdirektivet omhandler noe nytt – en statlig pålagt lagringsplikt for å dekke statens behov for trafikkdata. Selskapene har ingen egeninteresse av at datalagringsdirektivet innføres i Norge og motsetter seg derfor noe som helst økonomisk ansvar for dette.»

Kripos peker på at det ikke er vurdert administrative og økonomiske aspekter ved å legge beslutningskompetansen hos domstolen. *Kripos* er videre skeptisk til at tilbyder skal kunne velge lagringsløsning fordi kostnadsvurderinger åpenbart vil ligge til grunn for valg av løsning. Kostnadsaspektet blir i følge *Kripo*t den drivende faktoren.

Politidirektoratet sier følgende:

> «Politidirektoratet vil bemerke at dagens løsning innebærer betydelige utfordringer, og *ikke* bør videreføres. I de senere årene har det vært gjentatte drøftelser mellom Politidirektoratet på den ene siden og tilbyderne på den annen side om hvilke kostnader som skal dekkes av tilbyderne og hvilke kostnader politiet skal dekke etter ekomloven § 2-8. Loven oppstiller et skille mellom investeringskostnader som tilbyder skal betale og driftskostnader som politiet skal betale, men verken lovtekst eller forarbeider til ekomloven omhandler spørsmålet om sondringen mellom drifts- og investeringskostnader. Det hefter således en betydelig usikkerhet rundt plasseringen av de vesentligste kostnadene, som omfangsmessig har økt i sterk grad i de senere år.»

Politidirektoratet sier videre:

> «Vi vil stille spørsmål ved om det er riktig at politiet helt eller delvis skal dekke tilbydernes kostnader ved å etterkomme offentligrettslige pålegg for å bekjempe kriminalitet».

Forsvarergruppen av 1977 peker på den betydelige omfangsøkning bruk, analyse og bevisføring knyttet til kommunikasjonsdata medfører for rettsprosessene. Det oppstår et spørsmål om hvorvidt eskalering av kompleksiteten i sakene står i samsvar med de samfunnsmessige gevinster. De peker også på tidsaspektet og utfordring mht å beramme tid.

NAV mener at dersom tilbyder må dekke kostnadene ved lagring vil disse påføres kundene, noe som er negativt. *NAV* mener en sentralisert finansieringsmodell må vurderes.

Domstoladministrasjonen peker på at de vil kunne oppleve økt arbeid med behandling av begjæringer om utlevering av data sammenlignet med hva som er tilfellet for Post- og teletilsynet i dag. De mener de vil få betydelige behov for dommer- og saksbehandlerressurser, og anslår behovet til ca 10 MNOK i året.

Politijuristene sier følgende:

> «I denne sammenheng har vi også en bekymring knyttet til eventuelle kostnader ved utlevering av informasjon. Dersom den enkelte tilbyder selv kan diktere sine egne betingelser, vil det i realiteten bli redusert til et kostnadsspørsmål om politi og påtalemyndighet innhenter informasjonen. (Etter det vi er kjent med er det

blant annet i ferd med å bli et problem i Sverige). Et alternativ vil etter vår vurdering være å pålegge den konsesjonsberettigede å dekke slike utgifter selv.»

Forbrukerrådet sier følgende:

«Det fremstår ikke klart for Forbrukerrådet hvordan datalagringen skal finansieres. Dersom ekomtilbyderne forutsettes å dekke kostnadene i henhold til en tilretteleggingsplikt kan det se ut til at forbrukerne betaler til ekomtilbyderne for at staten skal kunne lagre data til etterforskning av lovbrudd. En slik fordeling av utgifter knyttet til politiarbeid er etter Forbrukerrådets syn ikke forenlig med drift av statens forskjellige forpliktelser».

Politiets Fellesforbund sier følgende:

«Utgifter til innhenting av trafikkdata har økt kraftig de senere årene. Dette er i takt med kriminalitetsutviklingen med stadig større innslag av organisert og annen alvorlig kriminalitet. Det er en kjensgjerning at erfaringsmessig store utgifter knyttet til dette ofte begrenser etterforskningen, fordi disse utgiftene gjør store innhugg i driftsbudsjettene. PF mener det er viktig at Ekomloven endres slik at trafikkdata kan innhentes vederlagsfritt fra teletilbyderne. Vi mener at dette i et samfunnsøkonomisk perspektiv vil være både ressursbesparende og effektivt. Alternativt bør det innføres en sentral refusjonsordning lik den som finnes i dag for sikring av DNA spor og analyser av disse.»

LO sier følgende:

«Uansett valg av løsning vil det bety økte kostnader for tilbyderne, myndighetene og brukerne. Dersom det pålegges en ny lagringspraksis som ikke er nødvendig for produksjon av tjenesten, og som betyr økte kostnader, framstår det som rimelig at myndighetene bevilger det som er nødvendig, på samme måte som i Finland, der justismyndighetene bekoster lagringsutvidelsen.»

NITO påpeker at på grunn av at ikke alle tilbydere per i dag har etablert systemer for lagring og uthenting, må eventuelle merkostnader dekkes av myndighetene. *TEKNA* påpeker at mindre tilbydere ikke har systemer og vil påføres større kostnader, noe som er konkurransevridende.

Abelia og *NHO* mener merkostnadene med tilbyders lagringsplikt bør dekkes av staten, da dette er en plikt som pålegges med bakgrunn i samfunnets ønske om å bekjempe kriminalitet.

NHO-reiseliv mener Norge bør følge det finske eksemplet og la den myndighet i hvis interesse lagringen skjer, dekke merutgiftene.

NorSIS mener kostnadsmodellene bør forsøkes å være likt i de nordiske land, som tilbyderne i størst mulig grad konkurrerer med. NorSIS sier videre

«Datalagringsdirektivet er omdiskutert med tanke på å sikre personvernet. NorSIS mener derfor det er vesentlig at Datatilsynet får økte og dedikerte ressurser, slik at de kan prioritere tilsyn av at trafikkdata er tilstrekkelig sikret og at tilbyderne sørger for å sikre persondata».

UNIO mener det må være myndighetenes ansvar, både økonomisk og administrativt, å sikre en forsvarlig og trygg lagring av trafikkdataene.

Universitetet i Oslo matematisk-naturvitenskapelige fakultet peker på at Teleplans analyse ikke tar høyde for kostnader forbundet med bedre sikring av data enn det som følger av minimumskravene.

16.5 Departementets vurdering

16.5.1 Nærmere om konsekvensene for myndighetene

Konsekvenser for politiet

Departementets forslag legger opp til en betydelig heving av lovens vilkår for å få utlevert data fra tilbyderne. Når retten har avgitt kjennelse om at lovens vilkår er til stede for uthenting, bør ikke eventuelle kostnader forbundet med uthentingen være en avveiningsfaktor når ansvarlig etterforsker beslutter om det skal innhentes data. Dette kan føre til at data ikke innhentes i saker som ellers er godt fundert for et videre etterforskningsarbeid med bruk av data. Det vises til Ot.prp.nr.19 (2006-2007) kapittel 3, om utvidet bruk av DNA-registrering i strafferettspleien, hvor kostnadselementet ved bruk av straffeprosessuelle virkemidler er problematisert.

Det må legges til grunn at bruken av data vil holde seg på tilsvarende nivå, eller øke, i uoverskuelig fremtid, noe som må tas i betraktning når det gjøres anslag over fremtidige kostnader. Det er departementets oppfatning at eventuelle kostnader for politimyndighetene på årsbasis bør ligge

innenfor rammen av kostnadsnivået i årene 2001-2007.

Konsekvenser for Post- og teletilsynet og Datatilsynet

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. Departementet foreslår at Post- og teletilsynets eventuelle økte kostnader dekkes gjennom kostnadsriktig justering av gebyrer, mens Datatilsynets økte kostnader som følge av datalagringsdirektivet bør kunne dekkes innenfor gjeldende budsjettrammer. Et eventuelt behov for styrking må vurderes i forbindelse med de årlige budsjettproposisjonene.

16.5.2 Nærmere om konsekvensene for tilbydere av ekomnett og -tjenester

Som det fremgår ovenfor viser Teleplans analyse at det for tilbyderne av ekomnett og -tjenester samlet vil koste 217 MNOK over en femårsperiode å innføre datalagringsdirektivet. 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. Analysen forutsetter at tilbyderne vil måtte etablere nye, egne systemer for lagring til kriminalitetsbekjempende formål, noe som er kostnadsdrivende. Departementet foreslår at det skal være opp til den enkelte tilbyder å finne egnet lagringsløsning. Noen tilbydere vil måtte investere i helt nye løsninger, mens andre tilbydere sannsynligvis vil se det som hensiktsmessig å bygge videre på eksisterende løsninger for lagring og uthenting. Hvilken løsning som velges er underordnet så lenge personvernet og informasjonssikkerheten til dataene ivaretas. Sikkerheten til data er svært viktig, og det må følgelig kunne forventes økte kostnader knyttet til sikkerhet.

Med dagens regler for kostnadsdeling vil kostnader for å få systemene på plass (investeringer) 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.

Ekombransjen peker i høringsrunden på de betydelige kostnadene de mener tilbyderne blir påført ved innføring av datalagringsdirektivet. Tilbyderne mener at dagens regler om tilrettelegging ikke automatisk kan videreføres og overføres til lagringsplikten. Departementet har merket seg ekombransjens synspunkter og har forståelse for bransjens bekymring om at de skal påføres kostnader for lagring og tilrettelegging. Departementet foreslår ingen lovendringer knyttet til kostnader ved innføring av datalagringsdirektivet. Dagens bestemmelse om kostnader knyttet til tilrettelegging for lovbestemt tilgang opprettholdes (jf. ekomloven § 2-8 annet ledd). Det er ikke tatt stilling til hvem som skal dekke kostnadene knyttet til lagringsplikten. Inntil videre skal dagens forståelse av gjeldende kostnadsmodell legges til grunn. En modell for hvordan kostnader skal beregnes og fordeles mellom ekomtilbyderne og justismyndighetene vil bli utarbeidet.

I arbeidet med en ny kostnadsmodell skal de samfunnsøkonomiske gevinstene ved innføring av datalagringsdirektivet beskrives nærmere, herunder hvordan de statlige utgifter skal kunne reduseres. Samfunnsøkonomiske gevinster kan blant annet omfatte mindre kriminalitet. Innføring av direktivet kan også medføre en mer effektiv saksbehandling i politiet. En redegjørelse for i hvilken grad teknologiutviklingen har gjort datalagring og uthenting av slik informasjon nødvendig for kriminalitetsbekjempelse og i hvilken grad datalagring gjør at politiet kan oppklare saker de ellers ikke ville oppklart, vil være nyttig for vurderingen av hvordan en eventuelt skal fordele kostnadene som lovpålagt datalagring medfører mellom myndighetene og tilbydere.

En kostnadsmodell skal utformes på en slik måte at tilbyderne og myndighetene i størst mulig grad tar hensyn til kostnadene som de påfører hverandre gjennom uthenting av data. Dersom tilbyderne for eksempel fikk dekket kostnadene knyttet til drift i forbindelse med datalagringen, ville tilbyderne prøve å minimere investeringskostnadene ved å øke driftskostnaden. Dette kunne for eksempel gjøres ved å investere i lavkvalitets datalagringsteknologi som krever store driftskostnader. Det ville heller ikke gi riktige incentiver om politiet og Finanstilsynet ikke skulle betale for uthenting av data. Dette kunne medføre at det samlet sett ble hentet ut lagrede data uhensiktsmessig mye i etterforskningen.

Innføring av standardpriser basert på kostnader knyttet til utlevering av data for en gjennomsnittlig ekomtilbyder er en modell som vil bli vurdert. Med en slik løsning vil tilbyderne ha incentiver til å drive kostnadseffektiv lagring. Politiet og Finanstilsynet på sin side ville internalisere kostnaden de påfører tilbyderne ved uthenting av data.

I utredningen skal det inngå en vurdering av om skillet mellom investeringskostnader og driftskostnader skal videreføres. Som det fremgår ovenfor vil tilbyderne for å oppfylle lagringsplikten måtte gjøre nye investeringer i sine nett og systemer. Disse investeringene vil måtte foretas før en endelig kostnadsmodell er på plass. Utredningen skal vurdere hvordan påløpte kostnader i perioden fra innføring av lagringsplikt til ny modell er på plass, skal fordeles. Utredningsarbeidet forutsetter at både politiet, tilbydere og de respektive myndigheter involveres i prosjektet. Et forslag til kostnadsmodell forventes å kunne foreligge innen utgangen av 2011.

16.5.3 Nærmere om konsekvensene for domstolene

Domstoladministrasjonen har i høringsrunden påpekt at forslaget om at politi- og påtalemyndighets begjæringer i fremtiden skal fremsettes for domstolene vil medføre en økning av domstolens saksmengde, hvilket især vil gjøre seg gjeldende for tingrettene. Domstoladministrasjonen er av den oppfatning at statistikken fremsatt over antallet begjæringer fremsatt for Post- og teletilsynet ikke kan tillegges nevneverdig vekt ved vurderingen av i hvilket omfang forslaget vil påføre domstolene økt saksmengde. Domstoladministrasjonen legger til grunn at økt mengde datavolum, lengre lagringstid og annet formål (kriminalitetsbekjempelse) tilsier økt arbeid sammenlignet med i dag. Domstoladministrasjonen mener at de mest åpenbare konsekvensene for domstolene vil være økt behov for dommer og saksbehandlerressurser og at departementets forslag samlet vil medføre en merkbar økning i domstolenes saksmengde, siden domstolene i realiteten overtar disse oppgavene fra Post- og teletilsynet. Videre vil Domstoladministrasjonen påføres en engangsutgift som følge av at funksjonaliteten i Lovisa må endres.

Etter departementets syn er det vanskelig å si med sikkerhet i hvilken grad domstolene påføres ekstraarbeid som følge av kravet om domstolsbehandling av utlevering av data. Dersom domstolenes arbeid viser seg å bli av et slikt omfang at det ikke kan dekkes innenfor gjeldende budsjettramme, vil behov for styrking av domstolsbudsjettet vurderes i samband med de årlige budsjettproposisjoner.

16.6 Oppsummert om administrative og økonomiske konsekvenser

Departementet er av den oppfatning at eventuelle kostnader for politimyndighetene på årsbasis bør ligge innenfor rammen av kostnadsnivået i årene 2001-2007. Post- og teletilsynets eventuelle økte kostnader foreslås dekket gjennom en kostnadsriktig justering av tilsynets gebyrer. Datatilsynets og domstolenes økte kostnader som følge av datalagringsdirektivet foreslås dekket innenfor gjeldende budsjettrammer. Dersom arbeidet viser seg å bli av et slikt omfang at det ikke kan dekkes innenfor gjeldende budsjettramme, vil behov for styrking av Datatilsynets budsjett og domstolsbudsjettet vurderes i samband med de årlige budsjettproposisjoner. Departementet foreslår at det utarbeides en modell for hvordan kostnader skal beregnes og fordeles mellom ekomtilbyderne og justismyndighetene. Arbeidet med denne modellen skal starte umiddelbart etter at saken er oversendt Stortinget. Det tas sikte på å utarbeide en forskrift om datalagring hvor denne modellen inngår.

17 Merknader til de enkelte bestemmelsene i lovforslaget

17.1 Merknader til endringer i straffeprosessloven

Til § 100 a første ledd første punktum

Henvisningen til § 210 d er ny. Paragraf 210 d hjemler utsatt underretning om utleveringspålegg som gjelder trafikkdata (forslaget til § 210 b) og basestasjonsdata (forslaget til § 210 c). Tilføyelsen innebærer at når retten behandler en begjæring om utleveringspålegg etter lovforslaget § 210 b eller § 210 c uten at mistenkte er underrettet, jf. § 210 d, skal vedkommendes rettsikkerhet ivaretas ved at det skal oppnevnes en offentlig advokat for vedkommende. Advokaten skal både sørge for kontradiksjon og være en rettssikkerhetsgaranti for at loven blir fulgt.

Henvisningen til ny § 210 f er en konsekvens av at gjeldende § 210 c om utsatt underretning om utleveringspålegg fremover i tid foreslås flyttet til ny § 210 f. Henvisningen innebærer følgelig ingen realitetsendring, men viderefører kravet om oppnevning av offentlig advokat ved utsatt underretning om utleveringspålegg fremover i tid.

Det vises til nærmere omtale av betydningen av denne bestemmelsen under kapittel 12.6.

Til ny § 118 a

Bestemmelsen retter seg mot enhver som er underlagt taushetsplikt i ekomloven § 2-9. Vilkårene for utlevering av lagringspliktig data etter straffeprosessloven §§ 210 b og 210 skal ikke kunne omgås ved bruk av vitneplikt i i straffesaker. Avgjørende for i hvilken grad retten kan ta imot et slikt vitneprov blir dermed i hvilken grad vilkårene for utlevering av data etter forslag til straffeprosessloven ny §§ 210 b og 210 c er oppfylt.

Det vises til nærmere omtale av betydningen av denne bestemmelsen under kapittel 12.6.

Til § 210 b:

Innholdet i bestemmelsen er nytt. Gjeldende § 210 b om pålegg om fremtidig utlevering er flyttet til ny § 210 e. Bestemmelsen regulerer utlevering av trafikkdata som er lagringspliktig i medhold av ekomloven § 2-7 a første ledd, og som etter gjeldende rett reguleres av den alminnelige bestemmelsen om utleveringspålegg i § 210. Utlevering av trafikkdata i etterforskningsøyemed skal etter forslaget ikke lenger kunne skje med hjemmel i § 210, ei heller med hjemmel i § 203 om beslag. Derimot er bestemmelsen ikke til hinder for at utlevering av trafikkdata fortsatt kan skje med hjemmel i § 216 b om kommunikasjonskontroll, jf. bestemmelsens annet ledd bokstav d, dersom vilkårene her er oppfylt.

Av *første ledd* følger det at virkeområdet for bestemmelsen er «trafikkdata, og lokaliseringsdata som ikke omfattes av § 210 c, og som tilbyder har plikt til å lagre etter lov om elektronisk kommunikasjon § 2-7a». Et grunnvilkår for pålegg om utlevering av slik data er at det foreligger skjellig grunn til mistanke om straffbar handling. Det kreves imidlertid ikke at mistanken retter seg mot noen bestemt. Den handlingen som kan gi grunnlag for utleveringspålegg etter bestemmelsen her må videre som utgangspunkt ha en strafferamme på fengsel i 4 år eller mer, jf. *bokstav a*. Dersom det er rimelig grunn til å tro at handlingen er utøvet som ledd i organisert kriminalitet, er det imidlertid tilstrekkelig at handlingen har en strafframme på fengsel i 3 år eller mer, jf. *bokstav b*. Uttrykket «grunn til å tro» skal forstås på samme måte som det tilsvarende uttrykket i straffeprosessloven § 215 a annet ledd om sikringspålegg og § 222 a første ledd om besøksforbud. Dette innebærer at det ikke kreves sannsynlighetsovervekt for at en slik handling er begått, jf. Ot.prp. nr. 109 (2001-2002) s. 44 og Ot.prp. nr. 40 (2004-2005) s. 35. Mistanken må imidlertid bygge på visse objektive holdepunkter i det konkrete saksforholdet, og kan derfor ikke utelukkende forankres i rent subjektive forestillinger. Bokstav b har betydning blant annet dersom det foreligger skjellig grunn til mistanke om simpelt tyveri, men uten at det også er sannsynlighetsovervekt for at tyveriet er utført som ledd i organisert kriminalitet.

Noe strafferammekrav gjelder likevel ikke dersom forholdet omfattes av en de straffebestemmelsene som er nevnt i *bokstav c*. Disse lovbrud-

dene kjennetegnes ved at trafikkdata anses særlig viktig i etterforskningen. Oppregningen er uttømmende.

Rettens beslutning om å pålegge utlevering skal treffes ved kjennelse. Kjennelsen må fastsette det historiske tidsrom som pålegget gjelder for og også de data som omfattes av pålegget. Tidsrommet kan ikke være lenger enn det som implisitt følger av kravet i tredje ledd om at dataene må være av vesentlig betydning for etterforskningen. Kravet om vesentlig betydning gjelder også i forhold til hvilke data som pålegget gjelder for.

Av *annet ledd* følger det at forhøyelse av strafferammen pga. gjentakelse eller konkurrens, jf. straffeloven 1902 §§ 61 og 62, ikke kommer i betraktning. Dette har bare betydning for pålegg om utlevering etter første ledd bokstav a eller b, da pålegg om utlevering etter bokstav c er uavhengig av strafferammen.

Tredje ledd innebærer et skjerpet krav til den antatte bevisverdien av trafikkdataene for at pålegg om utlevering skal kunne besluttes. Vilkåret om at opplysningene skal være av «vesentlig» betydning for etterforskingen, skal forstås på samme måte som det tilsvarende uttrykket i straffeprosessloven § 202 a første ledd. Det kreves ikke at utlevering av data skal være eneste mulige etterforskingsmetode i saken. Opplysningene må likevel på en kvalifisert måte være til hjelp for å avdekke de straffbare forhold, sikre bevis osv.

Av *fjerde ledd* følger det at første ledd annet punktum, annet og fjerde ledd i den alminnelige bestemmelsen om utleveringspålegg i § 210 gjelder tilsvarende. Henvisningen innebærer blant annet at påtalemyndigheten har hastekompetanse til å pålegge utlevering av trafikkdata dersom det å avvente rettens behandling medfører fare for at etterforskningen vil lide. Hastekompetansen er underlagt etterfølgende domstolskontroll.

Ved vurderingen av om det skal gis pålegg om utlevering av trafikkdata, gjelder kravet i straffeprosessloven § 170 a om at bruken av tvangsmiddelet i det konkrete tilfellet må være forholdsmessig og hensiktsmessig.

Det vises til nærmere omtale av bestemmelsen under kapittel 12.6.

Til § 210 c

Innholdet i bestemmelsen er nytt. Gjeldende § 210 c om unnlatt underretning om utleveringspålegg fremover i tid er flyttet til ny § 210 f. *Første ledd* regulerer utlevering av basestasjonsdata som er lagringspliktig i medhold av ekomloven § 2-7 a første ledd, og som etter gjeldende rett reguleres av den alminnelige bestemmelsen om utleveringspålegg i § 210. Utlevering av basestasjonsdata i etterforskningsøyemed skal etter forslaget ikke lenger kunne skje med hjemmel i § 210, ei heller med hjemmel i § 203 om beslag. Basestasjonssøk genererer gjennomgående store mengder overskuddsinformasjon. Utlevering skal derfor bare skje for et begrenset tidsrom.

Kravene til den handlingen som kan gi grunnlag for en begjæring om utlevering av data, er bygd opp på samme måte som forslaget til § 210 b første ledd bokstav a til bokstav c og det vises til merknadene til denne. Av personvernhensyn er strafferammekravet i bokstav a satt til fengsel i 5 år eller mer, mot 4 år eller mer i § 210 b bokstav a. Oppregningen i bokstav c er dessuten søkt avgrenset til handlinger som basestasjonssøk antas å være særskilt nyttig i etterforskningen av.

Annet ledd gir § 210 b annet til fjerde ledd tilsvarende anvendelse. Det vises til omtalen av disse bestemmelsene ovenfor. I forhold til basestasjonssøk vil kravet i § 210 b tredje ledd til «vesentlig betydning for etterforskningen» innebærer at pålegget må avgrenses i tid og sted, typisk på bakgrunn av åsted og antatt gjerningstidspunkt.

Straffeprosessloven § 170 a gjelder også for pålegg om utlevering av basestasjonsdata. Relevante momenter her vil blant annet være befolkningstettheten i det geografiske området det ønskes data fra, det straffbare forholdets alvorlighet og karakter, varigheten av det begjærte basestasjonssøket, og den tid på døgnet begjæringen knytter seg til.

Det vises til nærmere omtale av bestemmelsen under kapittel 12.6.

Til § 210 d

Bestemmelsen er et unntak fra hovedregelen om at «mistenkte eller andre som rammes» skal underrettes om utleveringspålegget, jf. straffeprosessloven § 208. Bestemmelsen svarer til den tilsvarende bestemmelsen i § 210 a om utsatt underretning om pålegg om utlevering av annet bevismateriale, jf. også gjeldende § 208 a om utsatt underretning om beslag og gjeldende § 210 c om unnlatt underretning om utleveringspålegg fremover i tid.

Kriteriet «rammes» skal forstås på samme vis som i straffeprosessloven § 210 a og § 377. Ved innhenting av data ved basestasjonssøk, vil ikke alle som det utleveres data om, bli ansett som «rammet» av utleveringspålegget. Å anses som

rammet utløser i tillegg til rett til å bli underrettet, også en selvstendig rett til å kreve domstolsprøving. Det forutsettes at vedkommende har en viss (faktisk) interesse i avgjørelsen.

Utsatt underretning kan bare besluttes hvis det er strengt nødvendig for etterforskningen at underretning ikke gis. Det skal altså mye til før underretning kan utsettes.

Beslutningen treffes av retten ved kjennelse. Den kan gå ut på at pålegg om utlevering av data kan settes i verk uten at den mistenkte eller andre varsles. Når retten mottar begjæringen om utsatt underretning, skal det oppnevnes offentlig advokat for den eller de som er mistenkt, jf. forslag til endring i straffeprosessloven § 100 a. Det vil på tidspunktet for beslutning om utlevering ikke nødvendigvis foreligge mistanke mot bestemte personer. Særlig gjelder dette ved pålegg om utlevering av basestasjonsopplysninger. I så fall vil det heller ikke være noen å oppnevne offentlig advokat for.

Det vises til nærmere omtale av bestemmelsen under kapittel 12.6.

Til §§ 210 e og f

Gjeldende § 210 b og § 210 c flyttes til ny § 210 e og § 210 f. Det tilsiktes ingen realitetsendringer. Som følge av ny nummerering endres henvisningen i *§ 210 f første ledd* til § 210 b, til § 210 e.

Til § 215 a femte ledd:

Denne bestemmelsen foreslås opphevet som overflødig ved siden av ny § 210 b.

17.2 Merknader til endring i politiloven

Til § 17 f nytt tredje ledd:

Første punktum er en henvisning til straffeloven 1902 § 121 om straff for brudd på taushetsplikt som følge av tjeneste eller arbeid for statlig eller kommunalt organ. *Annet punktum* innebærer at også personer som ikke er i tjeneste eller arbeid hos statlig eller kommunalt organ, for eksempel ansatte hos teletilbydere, vil kunne straffes etter straffeloven 1902 § 121 ved brudd på taushetsplikten. Straff for slike personer forutsetter imidlertid at de er blitt gjort oppmerksom på at brudd på taushetsplikten er strafflagt. Det er ikke oppstilt formkrav for underretningen, men den bør skje skriftlig.

17.3 Merknader til endringer i ekomloven

Til § 2-7 annet ledd

Bestemmelsen fastsetter hovedregelen om sletteplikt for trafikkdata, lokaliseringsdata og data som er nødvendige 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, og for data som er nødvendige for å identifisere abonnenten eller brukeren når slike data ikke er nødvendig av kommunikasjons- eller faktureringsformål. Sletteplikten gjelder ikke for telefonnummer, og faste IP-adresser. Telefonnummer og faste IP-adresser er eksempler på identifiseringsdata som er nødvendige både for kommunikasjonsformål og/eller for faktureringsformål.

Bestemmelsens ordlyd foreslås også endret som en konsekvens av innføring av plikt for tilbyder til å lagre data til bruk for bekjempelse av alvorlig kriminalitet. Lagringsplikten innebærer at tilbyder fremover både vil måtte lagre flere data og vil måtte lagre data i lenger tid enn det som er nødvendig for tilbyders egne kommunikasjons- eller faktureringsformål. Sletteplikten inntreden for en rekke data utsettes derved ut over det tidspunkt der tilbyder trenger data for egne legitime formål. Det følger derfor også som en konsekvens av formålet med lagringsplikten, at tilbyder må innføre egnede tiltak for å kontrollere tilgangen til data og at passende kontrolltiltak blant annet må sikre at tilbyder ikke selv nytter data etter dette tidspunkt. Det henvises i den sammenheng til merknaden til § 2-7a annet ledd og omtalen av tilbyders tilgangskontroll. Data som er lagret for å legge til rette for etterforskning og straffeforfølgning av alvorlige straffbare forhold, skal slettes samtidig med at lagringsplikten opphører. Bestemmelsen i § 2-7a går således foran bestemmelsen i personopplysningsloven § 28 om sletteplikt.

Til ny § 2-7a

Bestemmelsen er ny, og innfører lagringsplikt i en periode på 12 måneder for visse typer data. Innføring av en lagringsplikt skal sikre at definerte data skal være tilgjengelige for kompetente myndigheter i forbindelse med oppklaring, etterforskning og straffeforfølgelse av alvorlig kriminalitet. Det følger av sammenhengen mellom § 2-7 og § 2-7a at

tilbyder må sikre tilstrekkelig tilgangskontroll, som hindrer uautorisert tilgang og at data nyttes til formål som ikke er legitime.

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 tilfeller 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 data 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 benyttet og 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 brukers 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 brukers 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 og skal ikke lagres. Forslag til ny bestemmelse regulerer heller ikke forhold vedrørende utlevering av data. Utlevering reguleres blant annet av § 2-9 og av straffeprosesslovens regler. Lagringsplikten opphører etter 12 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 nr. 4 fremgår det at elektronisk kommunikasjonstjeneste er «tjeneste som helt eller i det vesentlige omfatter formidling av elektronisk kommunikasjon og som normalt ytes mot vederlag». Pliktsubjektet i § 2-7a er innsnevret i forhold til tilbyderdefinisjonen i ekomloven § 1-5 nr. 14, ved at det her stilles krav om «offentlig» elektronisk kommunikasjonstjeneste.

Når det gjelder offentlighetsbegrepet er det etter ekomlovens definisjon avgjørende om tjenesten er tilgjengelig for allmennheten eller beregnet til bruk for allmennheten, jf. § 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 annet 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. Dette betyr at den enkelte tilbyder kun skal lagre data om sine *egne* kunder.

Annet ledd inneholder en hjemmel for myndigheten til å fastsette nærmere regler om gjennomføringen av lagringen. Det foreslås innføring av en adgang for myndigheten til å gi forskrift, treffe enkeltvedtak eller inngå avtale om lagringsplikten der dette anses for hensiktsmessig. Det kan blant annet være relevant å utarbeide kvalitetskrav og tekniske standarder som skal gjelde i forbindelse med lagringen og uthenting av data fra tilbyders systemer. Det kan også være relevant å fastsette nærmere krav til tiltak som skal etablere den nødvendige sikkerhet i tilbyders systemer mot uhjemlet tilgang til de lagrede data. Det fremgår av formålet med lagringsplikten sammenholdt med bestemmelsen om kommunikasjonsvern i § 2-7, at når tilbyders tilgang til data ikke er nødvendig for kommunikasjons- eller faktureringsformål skal tilbyder etablere streng tilgangskontroll og gjennomføre nødvendige sikkerhetstiltak som hindrer utlevering av data til andre enn den kompetente myndighet for formål å bekjempe alvorlig kriminalitet, jf. også merknaden ovenfor til § 2-7 annet ledd. Tilgangskontroll kan gjennomføres ved etablering av et logisk skille enten i forbindelse med etablering av nye databehandlingssystemer eller ved tilpasning av tilbyders eksisterende systemer.

Myndigheten gis videre hjemmel til å kunne forvalte lagringsplikten slik at den virker etter sin hensikt. Det legges her opp til at myndigheten kan frita tilbydere som omfattes av tilbyderbegrepet i tredje ledd fra lagringsplikten. Adgangen til å frita for lagringsplikten er tenkt brukt i særlige tilfeller eller når anvendelse vil virke urimelig. Videre legges det opp til at myndigheten kan pålegge andre en hel eller delvis lagringsplikt. Dette kan i særlige tilfelle tenkes relevant for nødvendig oppfyllelse av det hensyn som ligger til grunn for innførsel av lagringsplikt. Ved vurderingen av 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 sluttbrukere knyttet til det elektroniske kommunikasjonsnett- eller tjeneste, om tilgangen ytes mot vederlag og tilbyders økonomiske forhold. Beskrivelsen er ikke uttømmende.

Til § 2-9 tredje ledd

Bestemmelsen første punktum om utlevering av identifikasjonsopplysninger til politi- og påtalemyndighet videreføres uendret uavhengig av taushetsplikten. Dette innebærer at slike opplysninger fortsatt kan utleveres til politiet uten at det er nødvendig med forutgående kjennelse fra retten eller Post- og teletilsynets fritak fra taushetsplikten. Det samme gjelder bestemmelsens andre punktum om vitnemål for retten der det heller ikke er nødvendig å innhente fritak. Et unntak fra dette er tvisteloven § 22-3 slik at det i sivile tvistemål må innhentes fritak fra departementet før opplysninger omfattet av første punktum kan tillates fremlagt som bevis for retten. Tredje punktum endres for å presisere 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. For andre taushetsbelagte opplysninger etter § 2-9 enn de som er nevnt i tredje ledd første punktum, kan det følgelig ikke bestemmes i annen lov at plikten til å gi opplysninger til offentlig kontrollorgan skal gå foran taushetsplikten, med mindre denne loven fastsetter at taushetsplikten ikke skal gjelde, og denne lovhjemmelen er inntatt i den uttømmende opplistingen i femte ledd. Videre kan retten fortsatt med hjemmel i tvisteloven kreve at denne type data utleveres av tilbyder til bruk som bevis under sivile søksmål.

Til § 2-9 nytt femte ledd

Bestemmelsen gjelder tilgang til data som i henhold til § 2-7 a er lagret for å legge til rette for etterforskning og straffeforfølgning av alvorlig kriminalitet. Taushetsplikten etter § 2-9 første ledd er ikke til hinder for at data som er lagret til disse formålene utleveres til påtalemyndighet og politi når retten har gitt tillatelse etter reglene i straffeprosessloven §§ 210 b, 210 c, 216 b eller 222 d, eller til Politiets sikkerhetstjeneste etter politiloven § 17 d. Tilsvarende gjelder utlevering av data til Finanstilsynet etter verdipapirhandelloven § 15-3 annet ledd nr. 3. Bestemmelsen i ver-

dipapirhandelloven, som gir Finanstilsynet tilgang til data tilsvarende politiets tilgang, gjennomfører internasjonale forpliktelser. I motsetning til tidligere praksis forutsetter myndighetens innhenting av data i disse tilfeller ikke at tilbyder først er fritatt fra taushetsplikten av Post- og teletilsynet. I alle andre tilfeller enn utlevering av opplysninger etter tredje ledd første punktum, forutsettes det at det foreligger lovhjemmel som gjør unntak fra taushetsplikten i denne bestemmelsen, og at lovhjemmelen er inntatt i opplistingen i femte ledd.

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

17.4 Merknader til endring i tvisteloven

Til § 22-3 nytt fjerde ledd

Bestemmelsen retter seg mot enhver som er underlagt taushetsplikten i ekomloven § 2-9 og knesetter et absolutt forbud mot føring av data som er lagringspliktig i medhold av forslaget til ekomloven 2-7 a første ledd, i sivile saker. Unntaket gjelder ikke abonnementsopplysninger og lignende som nevnt i ekomloven § 2-9 tredje ledd. For slike opplysninger gjelder de alminnelige bestemmelsene i tvisteloven § 22-3 første til tredje ledd om adgangen til å føre bevis om opplysninger undergitt lovbestemt taushetsplikt.

Vilkårene for utlevering av lagringspliktig data etter straffeprosessloven §§ 210 b og 210 skal ikke kunne omgås ved bruk av vitneplikt i sivile saker. Avgjørende for i hvilken grad retten kan ta imot et slikt vitneprov blir dermed i hvilken grad vilkårene for utlevering av data etter forslag til straffeprosessloven ny §§ 210 b og 210 c er oppfylt.

Det vises til nærmere omtale av bestemmelsen under kapittel 14.5.3.

17.5 Merknader til endring i verdipapirhandelloven

Til § 15-3 annet ledd nr. 3

Første ledd nytt annet punktum innebærer at Finanstilsynet må fremme begjæring for retten om tilgang til trafikkdata. Retten treffer beslutningen ved kjennelse, jf. *første ledd nytt tredje punktum.* Finanstilsynet har ikke kompetanse til å treffe vedtaket selv dersom det er fare ved opphold. Henvisningen til straffeprosessloven § 170 a innebærer at den generelle forholdsmessighets- og nødvendighetsvurderingen også skal foretas i en sak om utlevering av trafikkdata til Finanstilsynet, jf. *første ledd nytt femte punktum.* Straffeprosessloven § 170 a er nærmere omtalt i kapittel 12.6.

Den som rammes av utleveringen skal snarest mulig underrettes om kjennelsen, jf. *nytt annet ledd første punktum.* Terskelen for utsatt underretning etter straffeprosessloven § 210 a kommer tilsvarende til anvendelse for så vidt gjelder Finanstilsynets undersøkelser; og samtidig den korresponderende bestemmelsen i straffeprosessloven § 100 a om offentlig advokat, jf. *nytt annet ledd annet punktum.* Det vises til nærmere omtale av disse bestemmelsene i særmerknadene til forslaget til straffeprosessloven ny § 210 d samt i kapittel 12.6.

Forskriftshjemmelen er noe endret i tråd med at utlevering av trafikkdata heretter ikke lenger skal kunne skje uten rettens kjennelse, jf. *nytt annet ledd tredje punktum.* Forskriftshjemmelen berører flere departementers ansvarsområde og nærmere regler om domstolens samt Finanstilsynets behandling av saker om utlevering av trafikkdata til Finanstilsynet, må derfor utarbeides i samarbeid mellom disse. Innhenting av trafikkdata vil generere overskuddsinformasjon. Av personvernhensyn er det viktig at denne undergis en betryggende behandling. Nærmere regler om dette bør gis i forskrift, jf. den tilsvarende forskriftshjemmelen i verdipapirhandelloven § 15-5 femte ledd.

Det vises til nærmere omtale av bestemmelsen i kapittel 14.5.2.

17.6 Merknader til ikrafttredelsesbestemmelsen

Det er ønskelig at lovforslaget trer i kraft så snart som mulig. Av hensyn til tilbydernes behov for å tilpasse seg de krav lovforslaget stiller, foreslås det likevel at det nærmere ikrafttredelsestidspunktet fastsettes av Kongen. Det foreslås også gitt hjemmel for delt ikraftsettelse.

Ikrafttredelsen kan avdekke behov for nærmere overgangsregler. I nr. 2 åpnes det derfor for at Kongen i forskrift kan gi slike regler.

Justis- og politidepartementet

t i l r å r :

At Deres Majestet godkjenner og skriver under et framlagt forslag til proposisjon til Stortinget om lov om endringer i ekomloven og straffeprosessloven mv. (gjennomføring av EUs datalagringsdirektiv i norsk rett).

- - - - - - - - - - - - - -

Tilstedeværende statsråder fra Sosialistisk Venstreparti (statsrådene Halvorsen og Aasland) og tilstedeværende statsråder fra Senterpartiet (statsrådene Navarsete, Meltveit Kleppa, Riis-Johansen og Brekk) vil uttale:

«Etter en samlet vurdering har vi kommet til at vi ikke kan gi vår tilslutning til tilrådingen om gjennomføring av direktiv 2006/24/EF av 15. mars 2006 om lagring av data fremkommet ved bruk av elektronisk kommunikasjon (datalagringsdirektivet) i norsk rett. Vi legger særlig vekt på at datalagringsdirektivet etter vårt syn er en betydelig krenkelse av den enkelte borgers personvern.

Vi er bekymret for at systematisk, mer omfattende lagring av data enn i dag, 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. Vi er videre bekymret for at omfattende lagring av kommunikasjonsdata kan føre til at enkelte legger begrensninger på sin ytringsfrihet. Med store mengder kommunikasjonsdata lagret over lang tid, mener vi også faren øker for at dataene brukes til andre formål enn de er tiltenkt.

Vi mener dessuten at datalagringsdirektivet ikke er forholdsmessig og stiller spørsmål ved hvor egnet direktivet er til å nå formålet, og om det svarer til nytten for politiet. Vi viser til at nytten for politiet er omdiskutert og kjernen i EU-kommisjonens pågående evaluering av direktivet. Vi har en prinsipiell motstand mot omfattende lagring av opplysninger om alle borgere, og at tilbyderne pålegges å lagre data som de ikke selv har saklig behov for i sin virksomhet.

Vi vil også vise til at det i regjeringens politiske plattform slås fast at Sosialistisk Venstrepartis og Senterpartiets statsråder og stortingsrepresentanter stilles fritt i denne saken».

Vi HARALD, Norges Konge,

s t a d f e s t e r :

Stortinget blir bedt om å gjøre vedtak til lov om endringer i ekomloven og straffeprosessloven mv. (gjennomføring av EUs datalagringsdirektiv i norsk rett) i samsvar med et vedlagt forslag.

Forslag
til lov om endringer i ekomloven og straffeprosessloven mv. (gjennomføring av EUs datalagringsdirektiv i norsk rett)

I

I lov 22. mai 1981 nr. 25 om rettergangsmåten i straffesaker gjøres følgende endringer:

§ 100 a første ledd første punktum skal lyde:
Når retten behandler en sak etter §§ 200 a, 202 c, 202 e, 208 a, 210 a, *210 d, 210 f,* 216 a, 216 b, 216 m, 242 a, 264 sjette ledd, 267 første ledd tredje punktum eller § 292 a, skal den straks oppnevne offentlig advokat for den mistenkte.

Ny § 118 a skal lyde:
§ 118 a. Retten kan bare ta imot forklaring fra et vitne som har taushetsplikt i medhold av ekomloven § 2-9 første og annet ledd om opplysninger som nevnt i §§ 210 b og 210 c såfremt vilkårene for utlevering av de aktuelle opplysningene er oppfylt.

§ 210 b skal lyde:
Retten kan ved kjennelse pålegge utlevering for et bestemt tidsrom av trafikkdata, og lokaliseringsdata som ikke omfattes av § 210 c, og som tilbyder har plikt til å lagre etter lov 4. juli 2003 nr. 83 om elektronisk kommunikasjon § 2-7 a. Pålegg kan gis når det foreligger skjellig grunn til mistanke om en eller flere straffbare handlinger
a) *som etter loven kan medføre straff av fengsel i 4 år eller mer, eller*
b) *som etter loven kan medføre straff av fengsel i 3 år eller mer og det er grunn til å tro at handlingen er utøvet som ledd i virksomheten til en organisert kriminell gruppe, jf. straffeloven § 60 a, eller*
c) *som rammes av straffeloven §§ 90, 91, 91 a, 94 jf. 90, 104 a annet ledd, 145 annet ledd, 145 a, 145 b, 162, 162 b, 162 c, 190 a, 201 a, 203, 204 a, 270 første ledd nr. 2, 317, jf. § 162, eller § 390 a, eller av utlendingsloven § 108 fjerde ledd.*

Forhøyelse av maksimumsstraffen ved gjentakelse eller sammenstøt av forbrytelser kommer ikke i betraktning.

Utlevering etter paragrafen her kan bare pålegges dersom det må antas at opplysningene vil være av vesentlig betydning for etterforskningen.

§ 210 første ledd annet punktum, annet og fjerde ledd gjelder tilsvarende.

§ 210 c skal lyde:
Retten kan ved kjennelse pålegge utlevering for et begrenset tidsrom av opplysninger om hvilke telefoner eller annet kommunikasjonsutstyr som innenfor et nærmere bestemt geografisk område har vært satt i forbindelse med bestemte telefoner eller kommunikasjonsutstyr og som tilbyder har plikt til å lagre etter lov 4. juli 2003 nr. 83 om elektronisk kommunikasjon § 2-7 a. Pålegg kan gis når det foreligger skjellig grunn til mistanke om en eller flere straffbare handlinger
a) *som etter loven kan medføre straff av fengsel i 5 år eller mer, eller*
b) *som etter loven kan medføre straff av fengsel i 3 år eller mer og det er grunn til å tro at handlingen er utøvet som ledd i virksomheten til en organisert kriminell gruppe, jf. straffeloven § 60 a, eller*
c) *som rammes av straffeloven §§ 90, 91, 91 a, 94 jf. 90, 104 a annet ledd, § 162, 162 b, 162 c,*

eller § 317, jf. § 162, eller av utlendingsloven § 108 fjerde ledd.

§ 210 b annet til fjerde ledd gjelder tilsvarende.

Ny § 210 d skal lyde:

Retten kan ved kjennelse beslutte at underretning om utleveringspålegg etter § 210 b og § 210 c til den mistenkte eller andre som rammes av utleveringspålegget, kan utsettes dersom det er strengt nødvendig for etterforskningen i saken at underretning ikke gis.

§ 208 a gjelder tilsvarende.

Gjeldende § 210 b og § 210 c blir ny § 210 e og § 210 f.

§ 210 f første ledd skal lyde:

Retten kan beslutte at underretning til den mistenkte om utleveringspålegg etter *§ 210 e* kan utsettes dersom det er strengt nødvendig for etterforskningen i saken at underretning ikke gis.

§ 215 a femte ledd oppheves.

II

I lov 4. august 1995 nr. 53 om politiet (politiloven) skal § 17 f nytt tredje ledd lyde:

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 straffes.

III

I lov 4. juli 2003 nr. 83 om elektronisk kommunikasjon (ekomloven) gjøres følgende endringer:

§ 2-7 annet ledd skal lyde:

Trafikkdata, *lokaliseringsdata og data nødvendig for å identifisere abonnenten eller brukeren* skal slettes eller anonymiseres så snart de ikke lenger er nødvendig

1. til kommunikasjons- eller faktureringsformål,
2. *for å oppfylle plikten etter § 2-7a til å lagre data eller*
3. *for å oppfylle andre krav fastsatt* i medhold av lov.

Annen behandling av *slike data* krever samtykke fra bruker.

Ny § 2-7a skal lyde:

§ 2-7a. Plikt til lagring av data

Tilbyder av elektronisk kommunikasjonsnett som anvendes til offentlig elektronisk kommunikasjonstjeneste og tilbyder av slik tjeneste skal lagre trafikkdata, lokaliseringsdata og data nødvendig for å identifisere abonnenten eller brukeren i 12 måneder til bruk for etterforskning, oppklaring og straffeforfølgning av alvorlige straffbare forhold. Plikten etter første punktum gjelder data som genereres eller behandles i tilbyders elektroniske kommunikasjonsnett ved bruk av fasttelefon, mobiltelefon, internettelefoni, internettaksess og e-post.

Myndigheten kan gi forskrift, treffe enkeltvedtak eller inngå avtale om plikten til å lagre data, herunder om tiltak for å ivareta dataenes konfidensialitet, integritet og tilgjengelighet. Myndigheten kan ved forskrift eller enkeltvedtak helt eller delvis frita fra plikten til å lagre data etter første ledd eller helt eller delvis pålegge andre enn de som omfattes av første ledd plikt til å lagre data dersom dette må til for å oppnå formålet med bestemmelsen.

§ 2-9 tredje ledd skal 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.

§ 2-9 nytt femte ledd skal lyde:

Taushetsplikten er heller ikke til hinder for at andre data enn de som er nevnt i tredje ledd, kan utleveres til politi og påtalemyndighet i medhold av straffeprosessloven §§ 210 b, 210 c, 216 b eller 222 d, eller til Politiets sikkerhetstjeneste i medhold av politiloven § 17 d, eller til Finanstilsynet i medhold i verdipapirhandelloven § 15-3 annet ledd nr. 3.

§ 2-9 nåværende femte ledd blir sjette ledd.

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

IV

I lov 17. juni 2005 nr. 90 om mekling og rettergang i sivile tvister (tvisteloven) skal § 22-3 nytt fjerde ledd lyde:

(4) Et vitne som har taushetsplikt i medhold av lov 4. juli 2003 nr. 83 om elektronisk kommunika-

sjon § 2-9 første og annet ledd kan ikke pålegges å føre bevis om opplysninger som tilbyder av elektronisk kommunikasjonsnett og -tjeneste har lagret til bruk for etterforskning, oppklaring og straffeforfølgning av alvorlige straffbare forhold og som ikke omfattes av § 2-9 tredje ledd.

V

I lov 29. juni 2007 nr. 75 om verdipapirhandel (verdipapirhandelloven) skal § 15-3 annet ledd lyde:

(2) Opplysningsplikten i første ledd gjelder ikke opplysninger som vedkommende ville vært forhindret fra å gi i straffesak. Opplysningsplikten gjelder likevel uten hinder av:

1. lovbestemt taushetsplikt som ellers påhviler ligningsmyndigheter, andre skatte- og avgiftsmyndigheter og myndigheter som har til oppgave å overvåke offentlig regulering av ervervsvirksomhet,
2. taushetsplikt som nevnt i lov om elektronisk kommunikasjon § 2-9 for så vidt gjelder opplysninger om avtalebasert hemmelig telefonnummer eller andre abonnementsopplysninger og elektronisk kommunikasjonsadresse, og
3. taushetsplikt som nevnt i lov om elektronisk kommunikasjon § 2-9 for så vidt gjelder opplysninger om trafikkdata, dersom det er gitt fritak fra slik taushetsplikt. *Begjæring om slikt fritak fra taushetsplikten fremsettes av Finanstilsynet for tingretten på det sted hvor det mest praktisk kan skje. Retten kan ved kjennelse gi tilbyder slikt fritak.* Ved vurderingen av om fritak skal gis skal det blant annet legges vekt på hensynet til taushetsplikten og sakens opplysning. *Straffeprosessloven § 170 a gjelder tilsvarende.*

   Retten sørger for at kjennelsen snarest mulig blir meddelt den mistenkte eller andre som rammes av at taushetsplikten oppheves. Straffeprosessloven § 210 a jf. § 100 a gjelder tilsvarende. Departementet kan i forskrift gi nærmere regler om *domstolskontroll og* Finanstilsynets behandling av saker etter denne bestemmelsen, herunder regler om *behandlingen av overskuddsinformasjon.*

VI

1. Loven gjelder fra den til Kongen bestemmer. Kongen kan sette i kraft de enkelte bestemmelsene til forskjellig tid.
2. Kongen kan gi nærmere overgangsregler.

Offentlige institusjoner kan bestille flere eksemplarer fra:
Departementenes servicesenter
Internett: www.publikasjoner.dep.no
E-post: publikasjonsbestilling@dss.dep.no
Telefon: 22 24 20 00

Opplysninger om abonnement, løssalg og pris får man hos:
Fagbokforlaget
Postboks 6050, Postterminalen
5892 Bergen
E-post: offpub@fagbokforlaget.no
Telefon: 55 38 66 00
Faks: 55 38 66 01
www.fagbokforlaget.no/offpub

Publikasjonen er også tilgjengelig på
www.regjeringen.no

Trykk: 07 Xpress AS 12/2010

MILJØMERKET
241 570
Trykksak