Innst. 275 L

(2010–2011)

Innstilling til Stortinget fra transport- og kommunikasjonskomiteen

Prop. 49 L (2010–2011)

Innstilling fra transport- og kommunikasjonskomiteen om endringer i ekomloven og straffeprosessloven mv. (gjennomføring av EUs datalagringsdirektiv i norsk rett)

Til Stortinget

1. Sammendrag

1.1 Innledning

Justisdepartementet legger i 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
- verdipapirhandelloven.

Formålet med datalagringsdirektivet

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 lokaliseringsdata 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 hensikt med lovforslagene er å sikre samfunnets behov for data som etterforskningsverktøy i bekjempelsen av alvorlig kriminalitet.

Situasjonen i dag

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

Ekomloven § 2-8 pålegger allerede i dag tilbyderne en tilretteleggingsplikt for å sikre politiets lovbestemte tilgang til informasjon om sluttbruker og elektronisk kommunikasjon. 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.

Om høringen

Samferdselsdepartementet, Justisdepartementet og Fornyingsdepartementet sendte 8. januar 2010 på høring et forslag til hvordan datalagringsdirektivet kan gjennomføres i norsk rett. 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.

Nærmere om høringen i saken går fram av de enkelte kapitler i proposisjonen, jf. kapitlene 5–16.

Menneskerettighetene

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

Kriminalitet

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 i proposisjonen.

Personvernutfordringer

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 i proposisjonen.

Konkurranse innenfor elektronisk kommunikasjon

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 i proposisjonen.

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 for data for å bekjempe kriminalitet, slik det kom frem i høringen. Samtidig er hensynet til personvernet søkt ivaretatt blant annet ved at det foreslås strenge krav til informasjonssikkerhet og sletting.

Om merknader til de enkelte bestemmelsene i lovforslaget kan det vises til kapittel 17 i proposisjonen.

Kontroll ved utlevering av data i etterforskningsøyemed

Det er foreslått innskjerpelser sammenlignet med dagens regler om utlevering av data til politi og påtalemyndighet i etterforskningsøyemed. Også for Finanstilsynet er det foreslått innskjerpelser ved at det innføres domstolskontroll ved utlevering av data.

Det foreslås ingen endringer i reglene om Politiets sikkerhetstjenestes tilgang til data i avvergende eller forebyggende øyemed.

Personvern

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.

Hensynet til personvernet søkt ivaretatt blant annet ved at det foreslås strengere regler for politiets tilgang til data.

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 i proposisjonen.

Hvem skal lagre data

Temaet er nærmere omtalt i kapittel 7 i proposisjonen.

Lagring av data fremkommet ved bruk av elektronisk kommunikasjon er 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.

Ekomlovens tilbyderbegrep er foreslått videreført i den pågående revisjonen av loven. 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.

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 i proposisjonen.

Det foreslås at plikten til å lagre data etter ekomloven ny § 2-7 a 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.

Hva skal lagres

Temaet er nærmere omtalt i kapittel 8 i proposisjonen.

Lovforslaget innfører en lagringsplikt for tilbydere av offentlig ekomnett og -tjenester, samtidig som det stilles strenge krav til informasjonssikkerhet og sletting.

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.

Det foreslås at ekomloven ny § 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 teletil-

synet. Uklarheter i direktivet og hvordan implementering rent teknisk skal kunne skje, vil kunne avklares i forskriften.

Departementet foreslår at ekomloven ny § 2-7 a fastsetter hvilke kategorier av data som skal lagres, mens detaljene foreslås nedfelt i forskrift. Dette gjelder data ved fasttelefoni, mobiltelefoni, bredbåndstelefoni, internettaksess og e-post.

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 utover 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, vil fremgå i forskrift.

Lagringstid

Temaet er nærmere omtalt i kapittel 9 i proposisjonen.

Som det fremgår av kapittel 8 i proposisjonen (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.

Datalagringsdirektivet foreskriver at lagringstiden skal være mellom seks måneder og to år. I dette tidsspennet foreslår departementet 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 imot 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.

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 i proposisjonen. 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.

Lagringssted og informasjonssikkerhet

Temaet er nærmere omtalt i kapittel 11 i proposisjonen.

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.

Departementet går i proposisjonen 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.

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 ekomloven ny § 2-7 a.

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.

Regler for tilsyn

Temaet er nærmere omtalt i kapittel 15 i proposisjonen.

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.

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 ny § 2-7 a 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 § 2-7 a, 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.

Regler for tilgang

Temaene utlevering av data i etterforskningsøyemed, utlevering av data i avvergende og forebyggende øyemed og regler for tilgang til data for andre, er omtalt i kapittel 12, 13 og 14 i proposisjonen.

Etter gjeldende rett om politiets hjemler for innhenting av elektronisk lagrede data er utgangspunktet 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.

Politiets behov for data for bekjempelse av alvorlig kriminalitet 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 i proposisjonen 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, jf. straffeprosessloven § 210 b og § 210 c. 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.

Når det gjelder andre myndigheters tilgang, fastholder departementet 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. kapittel 14.5.2 i proposisjonen.

Innhenting av trafikkdata kan utgjøre et alvorlig inngrep i privatlivet til den det gjelder, og departementet går inn for at Finanstilsynets hjemmel ikke skal omfatte flere typer data enn våre folkerettslige forpliktelser tilsier. Finanstilsynets tilgang til data gjelder således bare 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.

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.

Økonomiske og administrative konsekvenser

Temaet er nærmere omtalt i kapittel 16 i proposisjonen.

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.

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.

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.

2. Komiteens merknader

Komiteens flertall, medlemmene fra Arbeiderpartiet, Anne Marit Bjørnflaten, Susanne Bratli, Freddy de Ruiter, Anita Orlund, Magne Rommetveit og Ivar Skulstad, og fra Høyre, Øyvind Halleraker, Lars Myraune og Ingjerd Schou, viser til proposisjonen om endringer i ekomloven og straffeprosessloven mv. (gjennomføring av EUs datalagringsdirektiv i norsk rett). Det fremmes forslag til endringer i lov om elektronisk kommunikasjon, straffeprosessloven, politiloven, tvisteloven og verdipapirhandelloven.

Flertallet viser til at formålet med EUs direktiv om datalagring 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.

Flertallet mener dagens situasjon for politiets benyttelse av trafikkdata er uholdbar, ut fra både hensynet til personvern og effektiv kriminalitetsbekjempelse. Flertallet viser i den sammenheng blant annet til NOU 2009:1 og NOU 2009:15, samt at politiet i omtrent ti år har ønsket en klarere fremgangsmåte for innhenting av trafikkdata i etterforskningsøyemed.

Flertallet viser til at tilbydere av offentlig elektronisk kommunikasjonstjeneste eller -nett (ekomtilbydere) i Norge i dag lagrer data for egne kommunikasjons- og faktureringsformål. Lagrings- og utleveringspraksis varierer i stor grad mellom de ulike ekomtilbyderne. Systemene for hvordan trafikkdataene lagres er veldig ulike, omfanget av hva som lagres er forskjellig, og hvordan sikkerheten er rundt disse opplysningene, har også ujevn kvalitet. Eksempelvis lagrer de fleste mobiloperatører en del trafikkdata ut fra faktureringsformål, mens for eksempel GET ikke lagrer noen trafikkdata. I dag er derfor tilgangen til disse dataene tilfeldig.

Flertallet viser videre til at trafikkdata i dag er helt avgjørende i etterforskningen av alvorlig kriminalitet. Trafikkdata fra telefoni brukes av politi og påtalemyndighet blant annet til å avdekke kontaktmønstre, og brukes primært i saker med flere involverte, som narkotikaomsetning, grove ran, menneskehandel og annen organisert kriminalitet. Et eksempel på dette kan etter flertallets mening være «Op Broken Lorry», hvor et marokkansk narkotikanettverk i 2006 ble rullet opp av Kripos. Totalt ble 35 domfelt over hele Europa, og to av bakmennene ble i Norge idømt 21 års fengsel. Lokasjonsdata/celle-ID registrerer hvilken basestasjon mobiltelefonen koblet seg til ved starten av en samtale, ved sending av SMS eller datatrafikk på mobilen. Dette gir slik en pekepinn på hvor brukeren av mobiltelefonen befant seg på det aktuelle tidspunktet. Lokasjonsdata kan dermed brukes som bevis for oppholdssted, omtrent som bilder fra overvåkningskamera, vitneobservasjoner eller lignende.

Lokasjonsdata var blant annet brukt i Nokasdommen.

Lokasjonsdata regnes som svært personverninngripende, blant annet på grunn av at mye overskuddsinformasjon om uskyldige blir generert ved basestasjonssøk. Flertallet viser til at dette i regjeringens forslag håndteres ved å stille krav om høyere strafferamme (5 år) for å hente ut basestasjonsdata enn øvrige data. Internettrafikkdata er særlig relevant i

saker hvor lovbruddet helt eller delvis begås på nettet. Aktuelle eksempler kan være grooming og spredning av overgrepsbilder av barn. Flertallet viser til at lagring av informasjon som knytter IP-adresser til en bestemt abonnent, er avgjørende for i det hele tatt å kunne innlede etterforskning i disse sakene.

Flertallet viser til uttalelser fra PST under komiteens høringer om at Norge uten datalagringsdirektivet blir mer utsatt for terror, og at PST bruker trafikkdata i alle sine saker. Riksadvokaten har i sin høringsanledning til Samferdselsdepartementet påpekt at:

«[u]ten implementering av datalagringsdirektivet mister politiet og påtalemyndigheten et sentralt og viktig virkemiddel ved etterforskning og iretteføring av alvorlig kriminalitet. Det vil gi manglende rettssikkerhet i vid forstand for borgere som med rimelighet forventer at rettshåndhevende myndigheter løser sine oppgaver minst like godt i morgen som i dag. I stedet etableres et system som innebærer at kriminelle fritt kan kommunisere uten fare for at myndighetene i ettertid (selv kort tid etter) kan spore kontakten, hvilket er noe nytt ved vår kriminalitetsbekjempelse.»

Flertallet viser til foreløpige tall fra EUs pågående evaluering, som demonstrerer at politiet i det alt vesentlige etterspør data som er nyere enn 6 måneder, selv om det også etterspørres en del data frem til de er 12 måneder gamle. Bare unntaksvis etterspørres data eldre enn 12 måneder. I en britisk undersøkelse fremgår det at 85 pst. av de data som ble brukt, var mindre enn 6 måneder gamle. Undersøkelsen viste imidlertid også at data som var mellom 7 og 12 måneder gamle, ble brukt i de alvorligste sakene, fortrinnsvis drapssaker. Regjeringen fremhever at dette stemmer med norske erfaringer. Ulike land har innført ulik lagringstid, Sverige 6 måneder, men flest land (ni) har valgt 12 måneders lagringstid.

Flertallet vil peke på at politiet i dag tar beslag i de data som er lagret, uavhengig av om de er lagret som en følge av at sletteplikten er brutt. Dette betyr at dersom man sier at dagens rettslige tilstand skal bevares, samtidig som man følger opp med strengere tilsyn og utleveringskrav slik at det ikke lagres data ulovlig, vil politiets muligheter til å oppklare eller forhindre alvorlig kriminalitet eller terror bli dårligere enn i dag.

Flertallet peker på at det særlig trengs klarere regler for hvilke data som skal lagres og sikringstiltakene som omgir denne lagringen. Det er etter flertallets mening uholdbart at data, slik som celle-ID, i dag lagres uten hjemmel. Lagrede data bør også sikres vesentlig bedre enn i dag.

Flertallet viser til felles avtale mellom Arbeiderpartiet og Høyre om behandlingen av Prop. 49 L (2010–2011). Avtalens tekst er som følger:

«**Innledning**

Partene er enige om å gjøre endringer i norsk lovgivning om lagring og sletting av elektroniske trafikkdata som følger av herværende avtale. Denne avtalen innebærer også en gjennomføring av EUs datalagringsdirektiv i norsk rett. Dette styrker kampen mot alvorlig kriminalitet. Trafikkdata fra elektronisk kommunikasjon går nå fra å bli lagret av et kommersielt hensyn – fakturering – til et samfunnsmessig hensyn – kriminalitetsbekjempelse. I dag lagres trafikkdata i enkelte tilfeller uten lovhjemmel, ofte i for kort tid og i blant lengre enn tillatt. Regelverket partene har blitt enige om vil styrke personvernet på dette og andre områder.

Å delta i det europeiske justis- og politisamarbeidet er avgjørende for kriminalitetsbekjempelsen i Norge. Kriminaliteten kjenner ingen grenser. Det må gjenspeiles i politiets arbeidsmetoder og verktøy. Teknologien kan ikke reguleres kun gjennom nasjonal lovgiving, den er grunnleggende internasjonal. Etterforskning av internasjonale terrorhandlinger er et godt eksempel på det. Endringene som nå gjøres i ekomloven mv. sikrer at norsk politi får nødvendige verktøy og sikrer samtidig den enkeltes trygghet og personvern. Politiet har hittil ikke kunnet etterforske og oppklare en rekke alvorlig straffbare forhold fordi Norge har manglet et lovverk som sikrer nødvendig lagring av kundeidentitet bak IP-adresser. Partene sikrer nå et slikt lovverk. Ekomtilbydere pålegges en plikt til å lagre data som sier noe om hvilke kommunikasjonsmidler som har vært i kontakt, hvor kommunikasjonen har funnet sted, når og hvordan.

Disse lovendringene er samtidig et viktig bidrag for å ivareta personvernet. På svært kort tid er det blitt slik at teknologien gjennomsyrer hverdagen vår. Personvernet er i dag under press på mange områder i samfunnet. For å ivareta personvernet innføres det strenge regler for uthenting, oppbevaring og sletting av data. Eksempler på dette er 6 måneders lagringstid, at politiet må ha rettens kjennelse ved utlevering av data, høy strafferamme og sletteplikt. Samtidig forutsetter vi at Datatilsynet styrker sin kontrollvirksomhet med ekomtilbyderne.

Som følge av denne avtalen styrkes den enkeltes rettssikkerhet, personvern og trygghet.

1. Typer data

Partene slutter seg til regjeringens forslag om hvilke typer data som skal lagres. Lovendringen 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.

2. Lagringstid

Partene er enige om at data som skal lagres i medhold av datalagringsdirektivet, lagres i *6 måneder*. Hensynet til personvern tilsier at de relevante data ikke skal lagres lengre enn hva som er strengt nødvendig av hensyn til kriminalitetsbekjempelse. Lagringsplikten avløses av sletteplikt i medhold av § 2-7 annet ledd. Lagringstid er et av forholdene som skal være gjenstand for evaluering, jf. avtalens pkt. 10.

Lagringspliktsbestemmelsen ser etter dette slik ut (endringer i kursiv):

«§ 2-7 a. 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 *6* 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 gi forskrift om at tilbyder kan kreve fremlagt politiattest fra personer som skal behandle lagringspliktige data på tilbyderens vegne.* 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.»

3. Innskjerpelse av sletteplikten

Partene er enige om ytterligere tydeliggjøring av sletteplikten knyttet til lagringsplikten i forhold til det som kommer fram av forslaget til endringer i ekomloven § 2-7 med tilhørende særmerknad i Prop. 49 L (2010–2011). Sletteplikten kommer tydelig til uttrykk i forslag til endringer i ekomloven § 2-7 annet ledd. Overskriften bør endres for å avspeile dette. Overskriften i ekomloven § 2-7 skal lyde:

«§ 2-7. Kommunikasjonsvern mv. *Plikt til å slette data.»*

4. Ansvar for lagring

Partene er enige om at ekomtilbyderne selv skal ha ansvar for lagring. Partene har særlig vektlagt personvern- og sikkerhetsmessige hensyn når det ikke foreslås å etablere en sentral lagringsløsning. Det er da opp til den enkelte tilbyder å velge lagringsløsning. Små tilbydere kan også gå sammen om en felles lagringsløsning.

5. Sikringstiltak

a) Konsesjonsplikt

Partene er enige om å endre forskrift 15. desember 2000 nr. 1265 om behandling av personopplysninger (personopplysningsforskriften) slik at § 7-1 lyder:

§ 7-1. Konsesjonsplikt for behandling av personopplysninger i ekomsektoren

Behandling av personopplysninger for kommunikasjons- og faktureringsformål, samt for å oppfylle plikten til å lagre data i medhold av lov 4. juli 2003 nr. 83 om elektronisk kommunikasjon (ekomloven) § 2-7 a første ledd hos tilbydere av elektronisk kommunikasjonsnett som anvendes til offentlig elektronisk kommunikasjonstjeneste og tilbyder av slik tjeneste, er konsesjonspliktig etter personopplysningsloven.

Sanksjoner

Partene er enige om at det må knyttes sanksjoner til brudd på konsesjonsvilkårene fastsatt i medhold av personopplysningsloven.

Sanksjoner er straff i form av bøter eller fengsel, jf. personopplysningsloven § 48 og erstatning, jf. personopplysningsloven § 49.

I tillegg kan det ilegges administrative sanksjoner i form av overtredelsesgebyr for manglende regeletterlevelse, jf. personopplysningsloven § 46 eller tvangsmulkt for manglende oppfyllelse av pålegg om overtredelsesgebyr, jf. personopplysningsloven § 47.

b) Autorisering av personell

Partene er enig om at personer som på vegne av den enkelte ekomtilbyder skal behandle data som faller under lagringsplikten, skal godkjennes (autoriseres) av ekomtilbyderen i hvert enkelt tilfelle:

- Ved vurdering av om autorisasjon skal gis, og ved revurdering av om autorisasjon skal opprettholdes, følges gjeldende retningslinjer. Slike retningslinjer utformes av Datatilsynet og Post- og teletilsynet i fellesskap. Retningslinjene skal omtale behov for politiattest.
- Pålegg om taushet om det en person blir kjent med under behandlingen av lagringspliktige data, herunder etter at han fratrer sin stilling, samt undertegning av taushetserklæring.
- Ekomtilbyderen gjennomfører periodevise autorisasjonssamtaler med den autoriserte. Samtaler gjennomføres minst årlig, samt ved tiltreden og fratreden fra stilling.
- Ekomtilbyderen skal føre kontroll med at de personer som behandler data har god kunnskap om regelverket for tilgang til og beskyttelse av dataene.

c) Kryptering og lukket lagring

Partene er enige om at kryptering er et godt tiltak for å sikre dataenes konfidensialitet. Partene er enige om at Datatilsynet gis myndighet til å gi pålegg til tilbydere om å foreta kryptering av data som faller under lagringsplikten etter (ny) ekomlov § 2-7 a. Omfanget av krypteringen, herunder knyttet både til lagring og forsendelse, fastsettes nærmere av Datatilsynet i det enkelte pålegg. Det skal utarbeides forskriftsbestemmelser for kryptering, som skal tilfredsstille etablerte internasjonale standarder.

Partene er enige om at data undergis nødvendig sikring (lukket lagring):

- Krav om identitetskontroll ved innpassering til de lokaler hvor data lagres.
- Adgang til de lokaler hvor data lagres og tilgang til data som er omfattet av lagringsplikten gis kun til personell som har tjenstlig behov for adgang og tilgang og har autorisasjon til det.
- Lagringsmediet og omgivelsene rundt sikres fysisk, slik at uvedkommende ikke får adgang til området uten at det etterlater spor.
- Lagringsmediet sikres elektronisk («brannmur» mv.).
- Det skal ikke være anledning til eksternt å koble seg til lagringsmediet, dvs. at data ikke kan hentes ut «on-line».

– Enhver forsendelse av lagringspliktige data over landegrensene skal sikres ved at krypteringsteknologi anvendes. Nasjonal sikkerhetsmyndighet gir retningslinjer for hvilken krypteringsgrad som er nødvendig for å ivareta sikkerheten.

d) Krav til sporbarhet

Partene er enige om at enhver bruk av lagrede data skal kunne spores for å forhindre uautorisert bruk. Med dette menes at det i ettertid kan konstateres hva som er gjort i et dataanlegg/informasjonssystem, herunder hvem som har fått tilgang til opplysningene og at all elektronisk behandling av opplysninger, skal være sporbare.

e) Lagringssted

Partene er enige om at plikt for den enkelte tilbyder til å informere kunder om lagringsstedet bør inntas i forskrift 16. februar 2004 nr. 401 om elektronisk kommunikasjonsnett og elektronisk kommunikasjonstjeneste (ekomforskriften), jf. § 1-8 om avtalevilkårene (forskriftsendringsforslag i kursiv):

§ 1-8. Avtale

Tilbyder av elektronisk kommunikasjonsnett som anvendes til offentlig elektronisk kommunikasjonstjeneste og tilbyder av slik tjeneste skal tilby sluttbruker avtale for abonnementstjenester, herunder kontantkorttjenester. Avtalen skal blant annet omfatte opplysninger om:

1. tilbyders navn og adresse
2. avtalens omfang, herunder relevante opplysninger om nett og tjenester, kvalitetsparametre, vedlikeholdsvilkår og tidspunkt for tilknytning
3. pris samt hvor man får tilgang til oppdatert informasjon om pris
4. avtalens varighet og vilkår for fornyelse og opphør
5. *sted for lagring av lagringspliktig data i medhold av ekomloven § 2-7 a*
6. kompensasjons- og refusjonsordninger ved kvalitetsavvik eller ved manglende levering
7. prosedyre for klagebehandling.

Tilbyder av elektronisk kommunikasjonsnett som anvendes til offentlig elektronisk kommunikasjonstjeneste og tilbyder av slik tjeneste skal etter ekomloven § 2-4 annet ledd varsle om endring i avtalen minst en måned før endringer iverksettes. Varslingsplikten gjelder endringer som må antas å ha en viss betydning for bruker*, men uansett for flytting av lagringssted for lagringspliktig data til en annen stat.* Dersom endringen er til ugunst for bruker skal bruker samtidig gjøres oppmerksom på adgangen til vederlagsfritt å kunne heve avtalen.

Annet ledd kan fravikes ved avtale utenfor forbrukerforhold.

Det tas forbehold for så vidt ikke internasjonalt regelverk er til hinder for å pålegge tilbyderne å opplyse om lagringssted.

6. Vilkår for utlevering av trafikkdata

Partene slutter seg til regjeringens forslag om strafferammer som ett av vilkårene for å få tilgang til data i etterforskningsøyemed. Dette 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 vanskelige å etterforske uten tilgang til data.

I dag er det ingen krav til den straffbare handlingens alvorlighetsgrad. Med denne lovendringen blir terskelen for å hente ut trafikkdata derfor vesentlig høyere. Strafferammekrav sikrer at innhenting av data bare kan skje i forbindelse med etterforskning av alvorlig kriminalitet.

7. Domstolsbehandling

Partene er enige om at begjæring om utlevering av trafikkdata skal domstolsbehandles. For at domstolene, som med dette blir tillagt nye oppgaver, sikres nødvendig kompetanse innen personvern og tekniske spørsmål, skal regjeringen sørge for at det gjennomføres kompetansehevende tiltak.

For å sikre at hastebestemmelsen ikke brukes unødig mye, skal én domstol ha en vaktordning, for å sikre kontinuitet og tilgjengelighet hos domstolene. Den nødvendige lovbestemmelsen foreslås nedfelt i tilknytning til bestemmelsene om utlevering av data i etterforskningsøyemed i straffeprosessloven ny §§ 210 b og 210 c, jf. følgende forslag:

«§ 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.

Utenfor domstolenes ordinære kontortid fremsettes begjæringer om utlevering for Oslo tingrett etter nærmere bestemmelser gitt av departementet.

§ 210 annet og fjerde ledd gjelder tilsvarende.»

«§ 210 c skal lyde:

Retten kan ved kjennelse pålegge utlevering for et begrenset tidsrom av opplysninger om hvilke tele-

foner 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 *femte* ledd gjelder tilsvarende.»

Hastekompetansen for påtalemyndigheten følger av § 210 b femte ledd jf. § 210 annet ledd og er subsidiær i forhold til å begjære rettens samtykke uavhengig av om det er tale om samtykke fra den stedlige rett eller fra vakthavende Oslo tingrett. Dette gjelder tilsvarende for basestasjonssøk, jf. § 210 c annet ledd og henvisningen til § 210 b femte ledd.

Partene er enige om at det skal føres statistikk over bruken av beredskapsordningen og hastebestemmelsene. Bruken av hastebestemmelsene er et av de forholdene som skal være gjenstand for en evaluering, jfr. avtalens pkt. 10.

8. Politiregisterloven

Partene er enige om at lov om behandling av opplysninger i politiet og påtalemyndigheten (politiregisterloven) og endringer i ekomloven og straffeprosessloven mv. (gjennomføringen av EUs datalagringsdirektiv i norsk rett) trer i kraft samtidig, og senest 1. april 2012. De elementer av politiregisterloven som gjelder logging og registrering av politiets bruk av data, forutsetter betydelige endringer i politiets IKT-systemer. Partene er enige om at fornyelse av politiets IKT-systemer skal prioriteres og følges opp, slik at gjenstående elementer i politiregisterloven kan tre i kraft raskt.

9. Datatilsynet

Partene er opptatt av at personvernet styrkes ved disse endringene i ekomloven mv. Datatilsynet fører i dag kontroll etter personopplysningsloven.

Partene er enige om behovet for at Datatilsynet styrker sin kontrollvirksomhet rettet mot ekomtilbydere og justissektoren/politiet betydelig, herunder overholdelse av sletteplikt, lagringstid og sikring av lagrede data, inkludert lagringssted.

Partene legger til grunn at ekomtilbydernes behandling av lagringspliktige data vil bli gjenstand for særlig oppmerksomhet i Datatilsynets tilsynsvirksomhet.

10. Evaluering

Lovforslagets siktemål er å imøtekomme behovet for data i kriminalitetsbekjempelsen og å sikre personvernet, blant annet ved strengere regler for politiets tilgang til data.

Reglene skal anvendes på et teknologisk område som er i stadig utvikling. Lagring og utlevering av data utfordrer dessuten personvernet.

Partene er derfor enige om at det etter en periode på fire år etter ikrafttredelsen skal foretas en evaluering for å undersøke om lovgivningen og tilhørende forskrifter har virket etter sin hensikt.

Følgende punkter bør inkluderes i en slik evaluering:

– Politiets bruk av hastekompetanse
– Lagringstid
– Vilkårene for utlevering av data i etterforskningsøyemed
– Erfaringer med domstolskontroll
– Lagringssikkerhet og personvern hos både ekomtilbydere og politiet
– Konkurransesituasjonen i ekommarkedet
– Eventuelle andre relevante forhold.
– Evalueringen skal legges frem for Stortinget på egnet måte senest fem år etter ikrafttredelse.

11. Videre arbeid

Partene er enige om at forskrifter skal utformes i tråd med intensjonen i denne avtalen.

Partene er enige om at hvis det i perioden fremlegges forslag til revisjon av datalagringsdirektivet skal Stortingets Europautvalg konsulteres.

12. Styrking av det generelle personvernet

Partene er enige om at personvernet skal styrkes på en rekke samfunnsområder. Partene legger til grunn at regjeringen som ledd i oppfølgingen av Personvernkommisjonens rapport, legger fram en stortingsmelding om personvern. Et grunnleggende personvernprinsipp er den enkeltes kontroll over egne personopplysninger og retten til å vite hvilke opplysninger andre behandler og hvem disse opplysningene overføres til. Partene ber derfor regjeringen i stortingsmeldingen særlig drøfte dette prinsippet og hvordan det kan ivaretas, blant annet gjennom logging av hvem som får tilgang til opplysningene og den enkeltes innsyn i disse loggene.

Partene er enige om at et grunnleggende prinsipp er at enhver har rett til innsyn i hvem som får tilgang til opplysninger om en selv. Plikten til logging og retten til innsyn i egen logg skal være det bærende prinsipp for alle større offentlige og private registre. I den avtalte stortingsmeldingen om personvern skal det drøftes hvilke avgrensninger som bør gjøres i loggplikten, innsynsretten, omfanget av innsynet i det enkelte forhold og framdriften i arbeidet med å virkeliggjøre prinsippet. Arbeiderpartiet viser her til unntaket for skattelistene.

Partene er også enige om å sikre personvernet gjennom å:

a) Be regjeringen sikre at det legges til rette for loggføring av interne oppslag i personregistre med sensitive personopplysninger i NAV, jf personopplysningsloven med forskrifter, og i behandlingsrettede registre i helsevesenet, jf helseregisterloven.
b) Legge til grunn at regjeringen sikrer at den registrerte gis innsyn i logg fra behandlingsrettet helseregister om hvem som har hatt tilgang til helseopplysninger om ham eller henne, det vil si innsyn i blant annet journal- og informasjonssystemer, jf helseregisterloven.
c) Ber regjeringen sørge for at det etableres syste-

mer for logging av elektroniske spor ved all tilgang til Norsk pasientregister (NPR), som forutsatt i forskrift om innsamling og behandling av helseopplysninger i Norsk pasientregister (NPR), hjemlet i helseregisterloven. Det skal også være utarbeidet oversikt over hvem som har fått utlevert opplysninger fra NPR, samt hjemmelsgrunnlaget for utleveringen. Oversikt over utleveringer skal også være utarbeidet for de øvrige sentrale helseregistrene.

d) Sikre at Arbeids- og velferdsetaten fortsatt avskjæres fra å innhente trafikk- og lokaliseringsdata fra elektronisk kommunikasjon, jf. Prop. 49 L (2010–2011).
e) Be regjeringen i forbindelse med framlegging av egen stortingsmelding om Personvernsspørsmål gjennomgå og vurdere rutiner og praksis for håndtering av taushetsbelagt informasjon i Arbeids- og velferdsetaten.
f) Følge opp trygdelovens bestemmelse om at NAVs mulighet til å innhente fullstendig journal kun gjelder ved mistanke om trygdemisbruk hos behandlende helsepersonell og sørge for at fullstendige journaler utelukkende behandles i Arbeids- og velferdsetatens særskilte kontrollenheter.
g) Viser til at det i henhold til politiregisterloven skal etableres en ordning med personvernrådgiver i justissektoren. Partene ber regjeringen sørge for at det etableres ordning med personvernrådgiver/-koordinator ved større statlige etater som behandler sensitive personopplysninger og at dette skal gjøres i NAV og helsesektoren.
h) Be regjeringen styrke ivaretakelse av arbeidstakernes personvern i arbeidsmiljølovens kapittel 9, slik at personvern synliggjøres i HMS-arbeidet.
i) I påvente av avklaring av muligheter for å begrense innsyn i lovlig lagrede data i elektroniske betalingsanlegg, er partene enige om at bomselskapene ikke skal utlevere passeringsopplysninger til ligningsmyndighetene.

13. Pressens kildevern

Partene er enige om at *pressens kildevern* er særdeles viktig i en tid der ny teknologi har skapt store utfordringer for personvernet. Partene har registrert at pressen er bekymret for at egen arbeidssituasjon vil bli vanskeligere med pliktig lagring av trafikkdata. Partene mener det er viktig å styrke journalistenes kildevern, og at en god måte å gjøre dette på er å oppstille begrensninger i adgangen til å avlytte telefoner eller lokaler som brukes av journalister, og til å bruke slike opptak som bevis. Partene er derfor enige om at de i forbindelse med behandlingen av Prop. 49 L (2010–2011) skal gi uttrykk for at det er behov for å endre straffeprosessloven § 216 m slik at journalister får et særskilt vern mot romavlytting, på linje med det som tilkommer avlytting av de øvrige yrkesgrupper som nå er nevnt i § 216 m fjerde ledd, og at man ber regjeringen fremme et slikt lovforslag som ledd i oppfølgningen av NOU 2009: 15.

14. Taushetsplikt

Partene er enige om at det er avgjørende for personvernet til de som opplever at trafikkdata om dem blir gjenstand for etterforskning, at de som i sitt arbeid kan få tilgang til slike data, har taushetsplikt. Partene er enige om at det i forbindelse med behandlingen av Prop. 49 L (2010–2011) skal gis uttrykk for at det er behov for å oppstille en *straffesanksjonert taushetsplikt for advokater,* og at man ber regjeringen fremme et slikt forslag som ledd i oppfølgningen av NOU 2009: 15.

15. Nødrett

Partene konstaterer at utlevering av data i nødrettssituasjoner ikke er lovregulert. Et krav til mistanke mot en konkret person kan være et problem for uthenting av data i en nødrettssituasjon. Blant annet derfor er kravet til mistanke i lovforslaget nå bare knyttet til skjellig grunn til mistanke om straffbar handling. Utlevering av data i nødrettssituasjoner som ikke oppfyller vilkårene i lovforslaget (straffeprosessloven §§ 210 b og 210 c) vil imidlertid fortsatt skje på ulovfestet grunnlag. Generelt innebærer utlevering på ulovfestet grunnlag muligheten for en rask innhenting av data i en nødrettssituasjon. På den annen side er lettere tilgjengelighet et argument for å lovfeste reglene.

Partene mener det vil være riktig å se nærmere på utformingen av en lovbestemmelse om dette. Utformingen må følge vanlig saksbehandling, herunder utredning og høring. Det er bl.a. viktig i lovarbeidet å sikre at utlevering bare skjer i de situasjoner hvor man mener de hensynene som tilsier det er tilstrekkelig tungtveiende. Det er uheldig både om man stenger noen muligheter ute eller favner for mange situasjoner.

Partene er enige om at et lovforslag om nødrett blir sendt på høring.

16. Forpliktelser for avtalepartene

Partene forplikter seg til å stemme for de konkrete budsjettmessige konsekvenser og de konkrete forslag som følger av avtalen.»

F l e r t a l l e t foreslår:

I lov om elektronisk kommunikasjon gjøres følgende endringer:

«Ny § 2-7 a skal lyde:

§ 2-7 a. *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 *6* 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 gi forskrift om at tilbyder kan kreve fremlagt politiattest fra personer som skal behandle lagringspliktige data på til-*

byderens vegne. 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.»

«Ny overskrift § 2-7 skal lyde:

§ 2-7. *Kommunikasjonsvern mv. Plikt til å slette data.»*

I lov om rettergangsmåten i straffesaker gjøres følgende endringer:

«§ 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.

Utenfor domstolenes ordinære kontortid fremsettes begjæringer om utlevering for Oslo tingrett etter nærmere bestemmelser gitt av departementet.

§ 210 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 *femte* ledd gjelder tilsvarende.»

«VI

I lov 14. april 2000 nr. 31 om behandling av personopplysninger (personopplysningsloven) skal § 35 nytt annet ledd lyde:

Ved behandling av personopplysninger som skal lagres etter ekomloven § 2-7 a skal det vurderes om det bør stilles vilkår om kryptering. Kongen kan ved forskrift gi nærmere regler om slik kryptering.»

Flertallet fremmer videre følgende forslag:

«B

«Stortinget ber regjeringen legge avtalen som den ligger i Innst. 275 L (2010–2011) til grunn for sitt arbeid med dette sakskomplekset.»

Flertallet har merket seg at komiteens mindretall hevder at:

«obligatorisk overvåkning av alle norske innbyggere slik datalagringsdirektivet legger opp til, representerer en massiv mistillit til landets innbyggere.»

Flertallet er skuffet over at komiteens mindretall ved en slik retorikk skaper unødvendig utrygghet hos folk. Flertallet vil understreke at lagring av historiske trafikkdata ikke innebærer overvåkning. Lagring av historiske trafikkdata skjer hos de fleste ekomtilbyderne alt i dag av kommersielle formål, som utarbeidelse av regninger. Lovverket for såkalt kommunikasjonskontroll, romovervåkning og fjernsynsovervåkning endres ikke ved denne saken. Flertallet registrerer også at komiteens mindretall utelukkende omtaler det såkalte datalagringsdirektivet, og ikke de konkrete lovendringene som foreslås i norsk rett.

Komiteens medlemmer fra Fremskrittspartiet, Jan-Henrik Fredriksen, Ingebjørg Godskesen, Bård Hoksrud og Arne Sortevik, fra Sosialistisk Venstreparti, Hallgeir H. Langeland, fra Senterpartiet, Janne Sjelmo Nordås, og fra

Kristelig Folkeparti, lederen Knut Arild Hareide, viser til at flertallet, bestående av Høyre og Arbeiderpartiet, legger fram omfattende lovendringer svært kort tid før komiteen har avsluttende behandling av innstillingen. Dette burde etter disse medlemmers syn medført en utsettelse av saken, slik at komiteen kunne gjennomgått konsekvensene av det fremlagte forslaget på en forsvarlig måte.

Disse medlemmer viser til spørsmål oversendt Justis- og politidepartementet og Samferdselsdepartementet 28. mars 2011, der det bes om svar på flere forhold vedrørende konsekvensene av avtalen mellom Høyre og Arbeiderpartiet, en avtale som ble kjent samme dag. Disse medlemmer konstaterer at det ikke har vært mulig for regjeringen å gi fyllestgjørende svar innenfor den fristen som flertallet, bestående av Høyre og Arbeiderpartiet, har satt for komiteens behandling av denne sak.

Disse medlemmer vil i den forbindelse vise til at den aller første setningen i Høyres prinsipprogram vedtatt av Høyres landsmøte 2008 lyder som følger:

«Høyre vil bygge samfunnet på tillit til enkeltmennesket.»

Disse medlemmer påpeker at obligatorisk overvåkning av alle norske innbyggere slik datalagringsdirektivet legger opp til, representerer en massiv mistillit til landets innbyggere. Disse medlemmer vil i den forbindelse vise til Kristin Clemets blogginnlegg på civita.no 11. mars 2011, som trekker frem følgende to sentrale problemstillinger:

«– Skal borgerne, i et fritt land, anses som potensielt skyldige inntil det motsatte er bevist – eller er de uskyldige inntil det motsatte er bevist?
– Skal staten kunne samle inn potensielle bevis mot borgerne i fall de begår en forbrytelse i fremtiden, eller er det en type politistat-metoder vi vanligvis ikke forbinder med et liberalt demokrati?»

Disse medlemmer viser til at det svenske parlamentet 16. mars 2011 utsatte implementeringen av datalagringsdirektivet i ett år, og at EU selv skal revidere datalagringsdirektivet i løpet av en måned. Disse medlemmer foreslår at implementeringen av datalagringsdirektivet utsettes til revideringen foreligger, og fremmer følgende forslag:

«Stortinget ber regjeringen utsette en eventuell implementering av datalagringsdirektivet til EUs revidering foreligger.»

Disse medlemmer viser til at datalagringsdirektivet betyr at alle innbyggere i Norge i praksis blir overvåket. Datalagringsdirektivet pålegger alle teleselskaper å lagre hvem man ringer til, hvor man ringer fra, hvor lenge man snakker, hvem man sender SMS til, hvor mottakeren befinner seg, når du er på Internett, hvor lenge, og hvem man sender e-post til.

Disse medlemmer mener at den type og det omfang lagring som datalagringsdirektivet krever, vil utgjøre både en stor trussel mot personvernet til norske innbyggere, og det vil bryte med det som hittil har vært viktige rettsstatsprinsipper. Samtidig er verktøyet betydelig mindre relevant og pålitelig mot kriminalitetsbekjempelse enn mange hevder.

Disse medlemmer går derfor imot implementering av direktivet i norsk lov.

Samtidig er ikke dagens datalagringsrutiner sikre nok i forhold til de personvern- og rettsstandarder som disse medlemmer mener bør gjelde for trafikkdata. Disse medlemmer vil derfor gå inn for innstramminger i dagens praksis mht. lagring og tilgang av trafikkdata, blant annet innføring av strengere regler for datakryptering samt domstolskontroll.

A. Begrunnelser for å gå imot datalagringsdirektivet

PERSONVERNHENSYN

Komiteens medlemmer fra Fremskrittspartiet, Sosialistisk Venstreparti, Senterpartiet og Kristelig Folkeparti påpeker at personvernet er under press, og ny teknologi muliggjør økt overvåkning. Ny teknologi innebærer alltid nye muligheter. Men det er politikkens rolle å sette grensene for teknologien når det finnes interessekonflikter; som her opp mot personvernet og rettsstatsprinsipper.

Datalagringsdirektivet endrer dagens praksis, fra en begrenset lagringsmulighet for faktureringsformål, til en pålagt lagring av trafikkdata over lengre tid. Direktivet pålegger alle teleselskaper å lagre hvem man ringer til, hvor man ringer fra, hvor lenge man snakker, hvem man sender SMS til, hvor mottakeren befinner seg, når man er på Internett, hvor lenge, og hvem man sender e-post til, i 6–24 måneder.

Overgangen fra lagringsmulighet og sletteplikt til en lagringsplikt, betyr et stort skritt inn i et overvåkingssamfunn som disse medlemmer ikke ønsker.

RETTSSTATSPRINSIPPER

Komiteens medlemmer fra Fremskrittspartiet, Sosialistisk Venstreparti, Senterpartiet og Kristelig Folkeparti viser til at bakgrunnen for EU-direktivet var den politiske situasjonen som oppsto i etterkant av terrorangrepet mot Madrid. Storbritannia, Sverige, Frankrike og Irland greide da å få flertall for et data-

lagringsforslag hvor hele Europas befolkning skulle overvåkes som om alle var potensielle terrorister.

Nå søkes direktivet innført i norsk lov. Med direktivet går man fra en situasjon hvor man overvåker på mistanke, til å betrakte alle innbyggere som potensielle lovbrytere. Å innføre datalagringsdirektivet er å legge det demokratiske rettsprinsippet om at enhver er uskyldig inntil det motsatte er bevist (uskyldspresumpsjonen), til side.

Disse medlemmer mener dette medfører noe helt nytt i norsk rettspraksis. Datalagringsdirektivet betyr ikke bare et stort skritt inn i et overvåkingssamfunn, men medfører også at man tråkker over en prinsipiell grense for selve rettsstaten.

Etterforskning

Komiteens medlemmer fra Fremskrittspartiet, Sosialistisk Venstreparti, Senterpartiet og Kristelig Folkeparti viser til at det har vært en debatt om i hvilken grad datalagringsdirektivet kan være et nyttig verktøy for politiet. Disse medlemmer har forståelse for at politiet ønsker tilgang til mer og bedre data. Men avveiningen om hvorvidt man mener de etterforskningsmessige fordelene man oppnår er verd de personvernmessige og rettsstatlige kostnadene direktivet har, er et politisk spørsmål, ikke et politispørsmål.

Det er i tillegg fullt mulig å sette store spørsmålstegn ved hvorvidt direktivet faktisk betyr økt nytte for politiet. Disse medlemmer viser til at politiet allerede i dag har vide fullmakter til å iverksette informasjonslagring ved berettiget mistanke om kriminalitet, blant annet for hendelser som ran, drap og forsvinninger.

Disse medlemmer vil samtidig påpeke at overvåkningen direktivet legger opp til, lett kan omgås ved å bruke proxy-servere, nettbasert e-post og falske e-postadresser, usikrede trådløse nett, Skype og andre teknologier.

Disse medlemmer viser til justisministerens svar av 28. mars 2011 på spørsmål 3, der det kommer frem at departementet ikke engang har fått med seg hvor lett der er å omgå direktivet. Disse medlemmer vil i den forbindelse som et banalt eksempel trekke frem at alle som har hjemme-PC-er fra Stortinget, har en VPN-tilknytning (virtuelt privat nettverk) som skjuler alle spor. Disse medlemmer er imot at uskyldige borgere skal settes under overvåkning.

Hensyn til barna

Komiteens medlemmer fra Fremskrittspartiet, Sosialistisk Venstreparti, Senterpartiet og Kristelig Folkeparti registrerer at overgrep mot barn har blitt ett av hovedargumentene for å få innført datalagringsdirektivet. Disse medlemmer viser til at Redd Barna konkluderer på følgende måte når det gjelder direktivet:

«Redd Barna spør seg om datalagringsdirektivet er svaret på de utfordringer man står overfor ved beskyttelse av barn på nettet. Vi mener det er behov for mer kunnskap om hvordan vi kan utnytte dagens muligheter og etterforskningsmetoder bedre, samtidig som vi etterlyser vurderinger av alternativer til datalagringsdirektivet.»

Disse medlemmer vil også vise til konklusjonen i Barneombudets høringsuttalelse:

«Basert på de henvendelser Barneombudet mottar, synes det som om politi og påtalemyndigheten har en rekke utfordringer knyttet til det å ivareta barns rettsikkerhet i straffesaker. Men årsaken synes ikke først og fremst å ligge i fraværet av Datalagringsdirektivet. Den ensidige fokuseringen på at det er Datalagringsdirektivet alene som skal trygge barn mot seksuelle overgrep synes ut fra dette noe søkt.

Et annet aspekt som Barneombudet ønsker å trekke frem er problemstillingen rundt hvilket samfunn vi ønsker å overlevere til våre barn. Når så tunge aktører som for eksempel Datatilsynet peker på farene for en glidning i retning av et overvåkningssamfunn, uavhengig av de eventuelle positive sidene ved Datalagringsdirektivet, må dette vektlegges.

Barneombudet ønsker også å fokusere på sentrale sider ved barns oppvekstmiljø i denne konteksten, ikke minst barns rett til privatliv og respekt for barns integritet. Disse spørsmålene er store og kompliserte, og Barneombudet finner derfor ikke grunnlag for entydig å konkludere med et barneperspektiv som skulle nødvendiggjøre implementeringen av Datalagringsdirektivet.»

Sverige utsetter

Komiteens medlemmer fra Fremskrittspartiet, Sosialistisk Venstreparti, Senterpartiet og Kristelig Folkeparti viser til at Sverige var blant de fire opprinnelige initiativtakerne til datalagringsdirektivet, og at Storbritannia, Sverige, Irland og Frankrike la frem et felles utkast til datalagringsdirektiv allerede i 2004. Disse medlemmer viser til at Sverige allikevel er blant landene som fortsatt ikke har innført direktivet, og at den svenske riksdagen 16. mars 2011 valgte å utsette implementeringen av direktivet i ett år til. Disse medlemmer understreker at Sverige ikke er det eneste landet i EU der implementeringen har gått i stampe. Den rumenske implementeringen av datalagringsdirektivet ble erklært grunnlovsstridig i 2009 og implementeringen reversert, og det samme skjedde i Tyskland i 2010. Disse medlemmer mener at det er paradoks at Arbeiderpartiet og Høyre er så ivrige etter å implementere et direktiv som i sin nåværende form neppe noensinne kommer til å bli implementert i samtlige EU-land.

Disse medlemmer viser til justisministerens svar av 28. mars 2011 på spørsmål 4, der det hevdes at problemene i Sverige og Tyskland knyttet til implementering av direktivet ikke vil påvirke Norges forpliktelser til å innføre datalagringsdirektivet etter EØS-avtalen. Disse medlemmer påpeker at flere anerkjente jurister har argumentert for at rettsakten ikke kan regnes som gjennomført i EU før samtlige EU-land har gjennomført den, og da at fristene knyttet til reservasjonsrett begynner å løpe. Disse medlemmer vil i den forbindelse vise til utredningen «Oversikt over mulige konsekvenser av norsk reservasjon mot EUs tredje postdirektiv» fra Kluge Advokatfirma 29. april 2010.

Til avtalen

Komiteens medlemmer fra Fremskrittspartiet, Sosialistisk Venstreparti, Senterpartiet og Kristelig Folkeparti viser til spørsmål fra komiteen til Justis- og politidepartementet datert 28. mars 2011 og departementets svar på disse datert 29. mars 2011. Disse medlemmer viser til at departementet blant annet bes uttale seg om de økonomiske konsekvensene knyttet til avtalen mellom Arbeiderpartiet og Høyre, herunder spørsmålet om domstolsbehandling og Datatilsynets nye oppgaver. Disse medlemmer viser til at departementet mener at en nærmere redegjørelse rundt disse spørsmål vil kreve en lengre tidsfrist enn det som er gitt i komiteens brev. Disse medlemmer bemerker at den korte fristen, som er satt av Høyre og Arbeiderpartiet, også medfører at departementet heller ikke kan gi svar på de andre tiltakene i avtalen som komiteen har forespurt om, det vil si evaluering og statistikk.

Disse medlemmer viser til avtalen mellom Arbeiderpartiet og Høyre der det foreslås en krypteringsordning. I svar fra Samferdselsdepartementet datert 29. mars 2011 svares det slik på komiteens spørsmål hva angår ulike sider ved kryptering:

«Den viktigste konsekvensen av forslaget om krav til kryptering er økte kostnader. Tilbyderne vil måtte implementere nye systemer, programvare o.l i sine allerede etablerte løsninger for kundehåndtering /fakturering. Dette vil bli svært dyrt.»

Disse medlemmer konstaterer at dette estimatet er det mest presise overslaget som nå er tilgjengelig.

Disse medlemmer viser til det oppsiktsvekkende og foruroligende svarbrevet fra Samferdselsdepartementet datert 29. mars 2011 der det heter at

«Oppsummeringsmessig vil forslagene i avtalen mellom Arbeiderpartiet og Høyre medføre svært høye kostnader og være meget utfordrende å gjennomføre. Belastningen for tilbyderne vil avhenge av modell for kostnadsdeling. Dersom tilbyderne må dekke kostnadene knyttet til kryptering vil dette kunne få store konsekvenser for tjenestetilbudet og konkurransen i markedet. I dag dekkes tilbydernes merkostnader til drift av staten. Dersom det innføres strengere krav til sikkerhet bør staten dekke kostnaden til dette.»

Disse medlemmer er bekymret for den praktiske gjennomføringen av avtalen mellom Høyre og Arbeiderpartiet. Disse medlemmer mener det ville vært behov for å gå nærmere inn på disse momentene før beslutninger fattes i en så viktig sak.

Komiteens medlemmer fra Fremskrittspartiet og Kristelig Folkeparti viser til at avtalen mellom Arbeiderpartiet og Høyre innebærer at datalagringsdirektivet i det alt vesentlige innføres i norsk rett slik Prop. 49 L (2010–2011) legger opp til. Disse medlemmer vil i den forbindelse påpeke at det ikke er foretatt noen endringer med hensyn til hvilke data som skal lagres, og at Arbeiderpartiet og Høyre derved setter hele befolkningen under kontinuerlig overvåkning gjennom systematisk registrering av befolkningens trafikkdata, epostkontakter, lokaliseringsdata og abonnments/brukerdata. Disse medlemmer har observert at Arbeiderpartiet og Høyre har forsøkt å fremstille forhandlingsresultatet som en personverneier som styrker den enkelts rettssikkerhet og personvern, og påpeker at man kunne ha oppnådd et langt bedre personvernresultat ved isteden å la være å implementere det omstridte direktivet.

Disse medlemmer viser til at datalagringsdirektivet spesifiserer seks måneder som korteste lovlige lagringstid, mens Arbeiderpartiet i Prop. 49 L (2010–2011) la opp til en lagringstid på tolv måneder. Disse medlemmer har hele tiden antatt at Arbeiderpartiet frontet en lengre lagringsperiode enn nødvendig for å ha noe å forhandle med andre partier om. Disse medlemmer er derfor ikke overrasket over at avtalen mellom Arbeiderpartiet og Høyre nå inneholder seks måneders lagringstid i henhold til direktivet. Kortere lagringstid enn utgangspunktet i Prop. 49 L (2010–2011) endrer imidlertid ikke på noen av de prinsipielle motforestillingene disse medlemmer har mot å sette hele befolkningen under døgnkontinuerlig overvåkning.

Disse medlemmer registrerer at avtalen mellom Arbeiderpartiet og Høyre inneholder et grunnleggende prinsipp om at enhver har rett til innsyn i hvem som får tilgang til opplysninger om en selv, blant annet personregistre med sensitive personopplysninger i Nav og i behandlingsrettede registre i helsevesenet. Disse medlemmer viser til at datalagringsdirektivet er en stort problem i forhold til pressens kildevern, fordi politiet i etterkant vil kunne finne frem til hvem som har hatt kontakt med den

enkelte journalist. Disse medlemmer viser til at politiet i en slik situasjon ikke har behov for verken romavlytting eller telefonavlytting for å finne frem til vitner og mistenkte, og at punktet om pressens kildevern i avtalen mellom Arbeiderpartiet og Høyre om å begrense muligheten til romavlytting av journalister bygger på en utdatert teknologiforståelse.

Disse medlemmer vil for øvrig understreke at transport- og kommunikasjonskomiteen har fått altfor liten tid til å sette seg inn i den fremforhandlede avtalen, og for liten tid til å innhente/bearbeide svar på spørsmål om avtalen og om konsekvenser/virkning av utsettelse i Sverige og Tyskland.

Komiteens medlemmer fra Fremskrittspartiet mener at det er oppsiktsvekkende at Høyre har gitt Arbeiderpartiet en blankofullmakt til å fortsette å publisere skattelistene, til stor glede for svindlere, kriminelle og mobbere.

Komiteens medlemmer fra Sosialistisk Venstreparti og Senterpartiet mener de budsjettmessige konsekvensene av avtalen mellom Høyre og Arbeiderpartiet ikke er godt nok redegjort før, selv om regjeringen ved Justis- og politidepartementet erkjenner at det påkommer økte kostnader på flere punkt. Disse medlemmer anser det som uaktuelt å støtte denne avtalen som man på en rekke områder ikke vet verken omfanget eller de budsjettmessige konsekvenser av.

B. Opplegg for datalagring

Komiteens medlemmer fra Fremskrittspartiet, Sosialistisk Venstreparti, Senterpartiet og Kristelig Folkeparti går imot forslaget om å pålegge lagringsplikt for mobiltelefonidata. Disse medlemmer vil videreføre dagens praksis med at selskapene ikke plikter å lagre informasjon (om hvor man ringer fra, hvem man ringer til, hvor man er når man ringer eller mottar samtaler osv.), men snarere at teleselskapene har en sletteplikt etter konsesjonstidens utløp. Dette betyr at selskapene kan lagre for faktureringsformål og selv sletter innenfor rammen av konsesjonsperioden (3–5 måneder) og lovgivning, som sier at data skal slettes etter at de er brukt til det formålet de var tiltenkt.

Disse medlemmer går imot forslaget om å innføre lagringsplikt for e-postinformasjon, slik direktivet krever (avsender, mottaker, avlogging, pålogging e-posttjeneste). Disse medlemmer mener at en lagringsplikt av slike data innebærer en prinsipiell endring fra før, nemlig at man ikke lenger er anonym på nettet. Teleselskapene er ikke pålagt å lagre dette i dag, men har konsesjon til lagring opptil 3 uker. Disse medlemmer ønsker å videreføre dagens praksis.

Disse medlemmer mener at det kan åpnes for pålagt lagring av IP-adresser i om lag 3 uker, som er dagens konsesjonstid. Dette er i tråd med Datatilsynets anbefalinger. En slik lovgivning må evalueres etter en periode, for å vurdere hvorvidt og eventuelt i hvilken grad lagringen av IP-adresser har ført til økt oppklaring, men også for å sammenligne med andre land som innfører en mer omfattende lovgivning.

Disse medlemmer mener at trafikkdata i framtiden bør lagres etter internasjonale sikkerhetsstandarder, inkludert krypteringssystem (jf. rapport ETSI TR 102 661).

Disse medlemmer mener at dagens praksis med å søke Post- og teletilsynet for tilgang til trafikkdata bør strammes inn. Disse medlemmer mener politiet kan få søke tilgang til dataene gjennom domstolskontroll med utsatt underretning (som blant annet Metodekontrollutvalget har tatt til orde for), unntatt ved hastesaker. En slik praksis vil medføre at den som er etterforsket uten å vite det, har en rettsbeskyttelse gjennom domstolene, samtidig som man sikrer at det må være proporsjonalitet i materialet som det bes om innsyn i.

Disse medlemmer mener det bør vurderes andre tiltak for å styrke arbeidet mot barneporno og seksuelle overgrep, for eksempel ved å styrke arbeidet ved KRIPOS.

Komiteens medlemmer fra Fremskrittspartiet og Kristelig Folkeparti er bekymret for den utviklingen man ser når det gjelder barneporno og seksuelle overgrep mot barn. Disse medlemmer registrerer at lovbrudd av denne typen ofte skjer gjennom nettverk med flere involverte. Det er derfor, etter disse medlemmers mening, viktig at politiets kamp mot denne type kriminalitet trappes opp og at politiet tilføres øremerkede ressurser i denne kampen.

Disse medlemmer er bekymret over den utviklingen en ser når det gjelder ID-tyveri. Dette problemet vil mest sannsynlig bare bli større. Disse medlemmer har merket seg at det er lett for kriminelle å skaffe til veie de opplysninger man trenger for å kunne stjele en annen persons identitet. Disse medlemmer mener at personnummer som sikker identifikasjon er gammeldags og lite hensiktsmessig, og vil at regjeringen skal utrede andre metoder for sikker identifikasjon.

Disse medlemmer viser til at EU arbeider med revisjon av datalagringsdirektivet (DLD) og med revisjon av EUs personvernlov. Disse medlemmer mener derfor at en evaluering fremlagt for Stortinget senest 5 år etter ikrafttredelse, slik Arbeiderpartiet og Høyre foreslår, er for lang tid dersom

DLD innføres av et flertall. Disse medlemmer fremmer følgende forslag:

«Stortinget legger til grunn at dersom DLD innføres, skal det gjennomføres en evaluering fremlagt for Stortinget senest 3 år etter ikrafttredelse der også konsekvenser av endring i EUs DLD og endring i EUs personvernlov inngår.»

Komiteens medlemmer fra Fremskrittspartiet ser at politiet har behov for ytterligere virkemidler i bekjempelsen av en kriminalitet som blir stadig grovere, mer avansert og mer utspekulert. Dette kan imidlertid avhjelpes uten DLD. Disse medlemmer vil derfor fremme forslag til tilpasninger som i større grad kan bidra til effektiv forfølgelse av kriminelle nettverk og andre som driver alvorlig kriminalitet. Disse medlemmer mener den største utfordringen i politiet nå er at etaten ikke er dimensjonert riktig i forhold til de utfordringer den står overfor.

Disse medlemmer ser at organisert kriminalitet i stadig større grad er med på å finansiere terror. Disse medlemmer mener dette er en alvorlig utvikling og vil derfor styrke overvåkningskapasiteten innen PST/politiet i Oslo. Etter disse medlemmers oppfatning er både kommunikasjonskontroll, kommunikasjonsavlytting, spaning og infiltrering, virkemidler det bør satses sterkere på. Dette er kostnadskrevende metoder, noe disse medlemmer tar inn over seg. Disse medlemmer mener dette er en pris man må betale. Disse medlemmer vil gi PST og politiet for øvrig økte ressurser til å prioritere slik overvåkning. Dette betyr også at PST skal gis flere ansatte som kan kvalifiseres til å drive nettopp denne typen virksomhet. Disse medlemmer viser til behandlingen av statsbudsjettet og Fremskrittspartiets alternative bevilgning til politiet i Innst. 6 S (2010–2011). Med 580 mill. kroner ekstra til politiet, derav 130 mill. kroner til politiet i Oslo, ville kapasiteten til å forfølge alle kriminalitetstyper vært mye større, og evnen til å kvele den organiserte kriminaliteten vært kraftigere og mer effektiv.

Disse medlemmer mener det tvinger seg frem et behov for strengere innvandringspolitikk og strengere registreringsrutiner ved asylankomst og ankomst av øvrige innvandrere, i bekjempelsen av terrorisme. Det er sannsynligvis bare en svært liten andel av innvandrerbefolkningen som er villig til å delta i terrorhandlinger, men jo flere innvandrere Norge mottar, jo større blir også terrorfaren. Disse medlemmer mener derfor at en generell innvandringspolitisk innstramming i seg selv kan bidra til å redusere terrorfaren. Disse medlemmer ser det som viktig å ha bedre kontroll ved Norges grenser. Disse medlemmer mener at god grensekontroll, både inn og ut av landet, er en viktig faktor for å begrense den organiserte kriminaliteten. I den forbindelse vil disse medlemmer gi tollvesenet begrenset politimyndighet samtidig som ressursene til tolletaten økes.

Disse medlemmer viser til at terrorisme i stor grad er et attraktivt verktøy for personer fra ekstreme islamske miljøer i visse land, og at Fremskrittspartiets utlendingslov i Innst. O. nr. 42 (2007–2008) åpnet for en differensiert innvandringspolitikk ut fra opprinnelsesland og de integreringsutfordringer innvandrere fra det aktuelle landet erfaringsmessig representerer. Dette ble gjort gjennom å innføre et nytt prinsipp om «integreringspolitiske hensyn» i utlendingslovgivningen. I praksis er dette imidlertid allerede langt på vei eksisterende politikk siden visumbestemmelser og EØS-regler fører til at ulike innvandrergrupper møter ulike regelsett.

Videre ønsker disse medlemmer å endre reglene i straffeprosessloven og politiloven slik at terskelen for å iverksette slik overvåkning mot mistenkte, potensielle terrorister blir lavere. Mer konkret vil disse medlemmer endre straffeprosessloven § 216 a-§ 216 d og § 216 m som gir adgang til å overvåke mistenkte kriminelle. I tillegg vil disse medlemmer endre politiloven § 17 d og e som hjemler PSTs adgang til forebyggende overvåkning i tilfeller der man mistenker planlegging av alvorlig kriminalitet.

På denne bakgrunn fremmer disse medlemmer følgende forslag:

«Stortinget ber regjeringen fremme forslag om styrking av overvåkningskapasiteten ved PST og Oslopolitiet.»

«Stortinget ber regjeringen gjennomgå straffeprosessloven §§ 216 a–216 d, 216 m samt politiloven § 17 d-e og legge frem forslag om endringer som senker terskelen for overvåkning av mulige terrorister.»

Disse medlemmer viser til at Fremskrittspartiet fremmet et komplett forslag til ny norsk utlendingslov i Innst. O. nr. 42 (2007–2008), der det ble åpnet for utstrakt bruk av DNA-testing i utlendingssaker. I § 42 og § 77 i Fremskrittspartiets lovforslag ble det åpnet for DNA-test i enhver utlendingssak der det er nødvendig å fastslå om det eksisterer en familierelasjon, og i § 90 ble det slått fast at det skal tas fotografi, fingeravtrykk og DNA-profil i forbindelse med en rekke andre utlendingssaker. Disse DNA-profilene skal lagres i et nasjonalt DNA-register som også skal kunne brukes i forbindelse med blant annet kriminalitetsbekjempelse. Disse medlemmer mener at et slikt register vil kunne være nyttig, og ikke bare når det gjelder å få registrert potensielle ter-

rorister, men også når det gjelder å spore opp personer som ikke selv er i registeret, men som har slektninger som har måttet gjennomgå slik DNA-test. PST skal ha tilgang til dette registeret, og forslagsstillerne mener man må foreta en vurdering av hvorvidt også andre deler av politiet bør ha det.

Disse medlemmer vil samtidig forby offentliggjøring av skattelister for å gjøre det vanskeligere for kriminelle å innhente opplysninger som senere kan benyttes som grunnlag for kriminell aktivitet.

Komiteens medlemmer fra Fremskrittspartiet, Sosialistisk Venstreparti, Senterpartiet og Kristelig Folkeparti viser til NOU 2009:1 Individ og Integritet – Personvern i det digitale samfunn; rapporten fra den såkalte personvernkommisjonen. Disse medlemmer minner om at rapporten inneholdt en egen uttalelse om DLD som siteres i sin helhet, men peker spesielt på følgende del av uttalelsen:

«Vi mener at datalagringsdirektivet setter både personvernet og ytringsfriheten på prøve. Dette vil gjelde selv om lagring av trafikkdata i henhold til direktivet ikke anses som kontinuerlig eller regelmessig overvåkning av borgerne. Verdien av lagring må nemlig også veies opp mot effekter på frimodighet. Dette gjelder selv om formelle friheter ikke berøres, og selv om de registrerte data kun skal være tilgjengelige for politiet under regulerte forhold. Allerede vissheten av at noen kan lete seg fram til dine kontakter og dine bevegelser, både i det virkelige rommet og på Internett, kan være nok til å hemme borgere i utøvelsen av sine friheter til å samles, til å ytre seg og til å søke opplysninger. Dette er grunnleggende rettigheter i et demokrati, som kommer til uttrykk både i norsk lovgivning og i Den europeiske menneskerettskonvensjon (EMK). Etter kommisjonens oppfatning vil innføring av direktivet kunne svekke opplevelsen av privatliv og privat kommunikasjon.»

Disse medlemmer viser til uttalelsen fra personvernkommisjonen i sin helhet:

«NOU 2009: 1 Individ og integritet

Personvernkommisjonen Juni 2008

Personvernkommisjonen har drøftet EU-direktiv 2006/24 (datalagringsdirektivet) og samlet seg om en felles uttalelse. Da forslag til innføring av direktivet i norsk rett ennå ikke er lagt frem, er våre kommentarer basert på direktivteksten.

Personvernkommisjonen har som mandat å vurdere hvordan personvernet bør ivaretas i møte med motstående hensyn og verdier. Personvernkommisjonen mener det må foretas en grundig utredning av konsekvensene for personvernet dersom direktivet blir iverksatt. Vi må også få en vurdering av konsekvensene dersom direktivet ikke innføres i Norge.

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 enkelte saker er det vanskelig for politiet å få tak i vitner. Tendensen er særlig tydelig innen organisert kriminalitet. I slike saker ser man at trafikkdata og elektroniske spor er svært sentrale bevis. Informasjonen er på mange måter et taust vitne og representerer i mange saker en tråd som lar seg følge. Men dersom det legges opp til pliktig lagring av trafikkdata, så vil det sannsynligvis forekomme ønsker/press fra ulike hold for å få tilgang til disse data.

Kredittilsynet og tollvesenet kan finne gode begrunnelser for at tilgang til trafikkdata vil bistå disse etatene i sitt arbeid. Helsevesenet kan argumentere for at kartlegging av sosiale kontaktnett gjennom trafikkdata kan redde liv og helse når man trenger å spore bærere av alvorlige smittsomme sykdommer. Nød- og redningsetater vil kunne argumentere for at trafikkdata vil kunne hjelpe dem med sporing av savnede personer. Personvernkommisjonen mener det er en reell fare for at pliktmessig lagring av trafikkdata med bekjempelse av alvorlig kriminalitet som formål etter hvert vil resultere i at disse data brukes til andre formål 1, som hver i sær kan være gode, men hvor den samlede bruken kan utgjøre en alvorlig trussel mot personvernet.

Personvernkommisjonens fokus er naturlig nok direktivets innvirkning på personvernet. Vi mener at datalagringsdirektivet setter både personvernet og

ytringsfriheten på prøve. Dette vil gjelde selv om lagring av trafikkdata i henhold til direktivet ikke anses som kontinuerlig eller regelmessig overvåkning av borgerne. Verdien av lagring må nemlig også veies opp mot effekter på frimodighet. Dette gjelder selv om formelle friheter ikke berøres, og selv om de registrerte data kun skal være tilgjengelige for politiet under regulerte forhold. Allerede vissheten av at noen kan lete seg fram til dine kontakter og dine bevegelser, både i det virkelige rommet og på Internett, kan være nok til å hemme borgere i utøvelsen av sine friheter til å samles, til å ytre seg og til å søke opplysninger. Dette er grunnleggende rettigheter i et demokrati, som kommer til uttrykk både i norsk lovgivning og i Den europeiske menneskerettskonvensjon (EMK). Etter kommisjonens oppfatning vil innføring av direktivet kunne svekke opplevelsen av privatliv og privat kommunikasjon.

EMK artikkel 8 annet ledd åpner for at det kan gjøres inngrep i personvernet. For at et slikt inngrep skal være forsvarlig må det blant annet være nødvendig i et demokratisk samfunn. I dette ligger det etter Den Europeiske Menneskerettighetsdomstolens (EMD) praksis at det må være en «pressing social need» for å gripe inn i personvernet. Det holder ikke at det er hensiktsmessig, rimelig eller ønskelig. Inngrepet som gjøres må dessuten være proporsjonalt i forhold til formålet som ønskes oppnådd. Den omfattende lagringsplikten som følger av direktivet kan etter Personvernkommisjonens oppfatning være problematisk i forhold til nødvendighetsprinsippet og proporsjonalitetsprinsippet. Forskning fra blant annet Tyskland 2 sår tvil om betydningen av trafikkdata for oppklaring av kriminalitet. Rapportene fra Tyskland omhandler selvsagt forhold knyttet til det tyske kriminalitetsbildet, og kan dermed ikke påberopes direkte i forhold til norske forhold. Kripos mener å ha erfaring for at trafikkdata har stor betydning for oppklaring av kriminalitet. Personvernkommisjonen etterlyser imidlertid en studie, tilsvarende den man har gjort i Tyskland, for norske forhold. Kriteriene som følger av EMK artikkel 8 krever etter kommisjonens oppfatning en grundig klargjøring i form av dokumentasjon av behovet for lagring (både lagringstid og omfanget av opplysninger) og en grundig konsekvensutredning: Både personvernmessige konsekvenser av en eventuell innføring og konsekvenser for politiet og kriminalitetsbildet dersom Norge ikke innfører direktivet. Personvernkommisjonen er usikker på om slik dokumentasjon eller utredninger ligger til grunn for direktivet eller for arbeidet som er gjort i forbindelse med en eventuell innføring av direktivet i norsk rett.

Det synes klart for Personvernkommisjonen at direktivet representerer noe nytt i forhold til dagens regime for lagring av trafikkdata. Direktivet innebærer for det første lagring av nye typer data , som for eksempel geolokaliseringsdata og epost-logger. For det andre vil direktivet medføre lengre lagringstid enn det som følger av dagens praksis. For det tredje berøres langt flere organisasjoner enn det som er dagens situasjon, blant annet omfatter direktivet mange ISPer. For det fjerde gir direktivet et nytt normativt grunnlag for lagring av trafikkdata – en plikt til å lagre for andre formål enn faktureringsformål. Det er også et moment at man går fra en rett til å lagre opplysninger for visse formål, til en plikt til å lagre opplysninger . Disse forholdene må hensyntas i vurderingen av om og eventuelt hvordan direktivet skal innføres i norsk rett.

Dersom direktivet skulle bli innført, mener kommisjonen at det er viktig at lagringstiden gjøres så kort som mulig. Personvernkommisjonen vil også peke på spørsmålet om hvilken sikkerhet man har for de opplysningene som lagres. Mye tyder på at mange organisasjoner ikke har fullgode mekanismer for sikring av trafikkdata mot uautorisert spredning. 3 Det har vært fremhevet som en trussel mot sikkerheten at tilbydere pålegges å lagre store mengder data på vegne av myndighetene, og at manglende egeninteresse i lagring av opplysningene til dette formålet vil kunne gå ut over sikkerheten. Dersom lagring i en så omfattende skala som direktivet legger opp til blir gjennomført, må det fra myndighetens side settes krav til sikring i form av kryptering og deponeringsmekanismer som hindrer at så vel teletilbyderen selv, som myndighetene, kan få tilgang til lagrede data før korrekt rettslig grunnlag for tilgang kan fremlegges. Det må også sikres at enhver tilgang som gis, avgrenses til de data det skal være lovlig tilgang til. Det er etter kommisjonens oppfatning avgjørende at en eventuell innføring av direktivet ledsages av sikringer – tekniske og organisatoriske så vel som juridiske – mot at det lagrede materialet kan brukes til strategisk informasjonsanalyse eller andre former for generell informasjonssøking. I forhold til den tekniske siden vil dette innebære at det må utvikles nye, finmaskede systemer for tilgangskontroll og datasikring som, så vidt Personvernkommisjonen har kjennskap til, ikke er tilgjengelig på markedet i dag.

Oslo 12. juni 2008

1. Våren 2008 ble det rapportert at Deutsche Telekom ulovlig hadde analysert trafikkdata i et forsøk på å identifisere en pressekilde, jf. Prosecutors investigate Deutsche Telekom over data misuse; 29. mai 2008, tilgjengelig på adresse: http://www.out-law.com//default.aspx?page=9153.; Overvåkingsskandalen vokser; 3. juni 2008, tilgjengelig på adresse: http://e24.no/utenriks/article2462382.ece.
2. Se: Max-Planck-Institut für ausländisches und internationales Strafrecht:Rechtswirklichkeit der Auskunftserteilung über Telekommunikationsverbindungsdaten nach §§ 100g, 100h StPO: Forschungsbericht im Auftrag des Bundesministeriums der Justiz (Freiburg, februar 2008); tilgjengelig på adresse: http://www.vorratsdatenspeicherung.de/images/mpi-gutachten.pdf, som hevder at trafikkdata kun vil bidra til oppklaring i et lite antall, anslagsvis 0,002 % av det totale antall kriminalsaker, og anslag fra det tyske Bundeskriminalamt, som ifølge en separat studie utført sommeren 2007 regner med at datalagring vil føre til en økning i oppklaringsraten «fra dagens 55 prosent, i beste fall til 55,006 prosent», jf. http://www.heise.de/newsticker/Vorratsdatenspeicherung-fuer-eine-0-006-Prozentpunkte-hoehereAufklaerungsquote--/meldung/92746.
3. Personvernkommisjonen viser til den såkalte Tele2-saken, hvor Tele2 våren og sommeren 2007 lot kredittopplysninger om et sekssifret antall personer tilflyte uvedkommende. En enda større skandale fant sted i Storbritannia høsten 2007, hvor to ukrypterte disker med personopplysninger vedrørende alle familier i Storbritannia med barn under 16 år kom på avveie. Se: Brown apologises for records loss, BBC News, 21.

november 2007, http://news.bbc.co.uk/2/hi/uk_news/politics/7104945.stm.

2.1 Uttalelser fra justiskomiteen og utenriks- og forsvarskomiteen

Utkast til innstilling fra transport- og kommunikasjonskomiteen har vært forelagt justiskomiteen og utenriks- og forsvarskomiteen til uttalelse.

Fra brev datert 29. mars 2011 fra justiskomiteen siteres:

«**Prop. 49 L (2010–2011) – justiskomiteens merknader**

Justiskomiteen viser til transport- og kommunikasjonskomiteens foreløpig avgitte innstilling datert 29. mars 2011 vedrørende Prop. 49 L (2010–2011) Endringer i ekomloven og straffeprosessloven mv. (gjennomføring av EUs datalagringsdirektiv i norsk rett).

Justiskomiteens medlemmer slutter seg til transport- og kommunikasjonskomiteens innstilling og sine respektive partiers merknader til proposisjonen og har ingen ytterligere merknader.

Komiteens medlemmer fra Fremskrittspartiet er lite tilfredse med den svært korte tiden som er satt av til justiskomiteens behandling av saken og vil bemerke at disse medlemmer ikke har fått satt seg inn i innstillingen.»

Fra brev datert 30. mars 2010 fra utenriks- og forsvarskomiteen siteres:

«**Utenriks- og forsvarskomiteens merknader**

Utenriks- og forsvarskomiteen viser til transport- og kommunikasjonskomiteens utkast til innstilling datert 29. mars 2011 og til de respektive partiers merknader vedrørende Prop. 49 L (2010–2011).

Utenriks- og forsvarskomiteens flertall, medlemmene fra Arbeiderpartiet og Høyre slutter seg til transport- og kommunikasjonskomiteens utkast til innstilling til Prop. 49 L (2010–2011) og har ingen ytterligere merknader.

Komiteens mindretall, medlemmene fra Fremskrittspartiet, Sosialistisk Venstreparti, Senterpartiet og Kristelig Folkeparti mener de budsjettmessige konsekvensene av avtalen mellom Høyre og Arbeiderpartiet ikke er godt nok redegjort for, selv om regjeringen ved Justis- og politidepartementet erkjenner at det påkommer økte kostnader på flere punkt. Disse medlemmer anser det som uaktuelt å støtte denne avtalen som man på en rekke områder ikke vet verken omfanget eller de budsjettmessige konsekvenser av.

Disse medlemmer viser til at avtalen mellom Arbeiderpartiet og Høyre setter siste frist for implementering til 1. april 2012. Innenfor en slik tidsramme vil det være rom for en mer forsvarlig behandling av saken fra Stortingets side.

EUs planlagte evaluering, med de muligheter for justeringer som ligger i denne, samt at gjennomføringen i andre land (utsettelsen i Sverige, implementeringen i Tyskland er grunnlovsstridig) peker klart i retning av at vi bør utsette behandlinga. Dette ville uansett ikke hatt noen konsekvenser for den datoen som Høyre og Ap har satt for implementeringen, april 2012.»

2.2 Korrespondanse mellom komiteen og Justis- og politidepartementet og Samferdselsdepartementet

I behandlingen av Prop. 49 L (2010–2011) i transport- og kommunikasjonskomiteen er det stilt en rekke spørsmål til Justis- og politidepartementet og Samferdselsdepartementet.

Komiteen viser til brev til Justis- og politidepartementet datert 13. januar 2011, 24. januar 2011, 1. februar 2011, 11. februar 2011, 21. februar 2011, 10. mars 2011, 23. mars 2011, 28. mars 2011, 28. mars 2011 (brev 2), og til svarbrev fra Justis- og politidepartementet datert 27. januar 2011, 28. januar 2011, 4. februar 2011, 18. februar 2011, 1. mars 2011, 17. mars 2011, 25. mars 2011, 29. mars 2011.

Komiteen viser til brev til Samferdselsdepartementet datert 11. februar 2011, 28. mars 2011, 28. mars 2011 (brev 2) og til svarbrev fra Samferdselsdepartementet datert 21. februar 2011, 29. mars 2011.

3. Forslag fra mindretall

Forslag fra Fremskrittspartiet, Sosialistisk Venstreparti, Senterpartiet og Kristelig Folkeparti:

Forslag 1

Stortinget utsetter en eventuell implementering av datalagringsdirektivet til EUs revidering foreligger.

Forslag fra Fremskrittspartiet og Kristelig Folkeparti:

Forslag 2

Stortinget legger til grunn at dersom datalagringsdirektivet (DLD) innføres, skal det gjennomføres en evaluering fremlagt for Stortinget senest 3 år etter ikrafttredelse der også konsekvenser av endring i EUs DLD og endring i EUs personvernlov inngår.

Forslag fra Fremskrittspartiet:

Forslag 3

Stortinget ber regjeringen fremme forslag om styrking av overvåkningskapasiteten ved PST og Oslopolitiet.

Forslag 4

Stortinget ber regjeringen gjennomgå straffeprosessloven §§ 216 a–216 d, 216 m samt politiloven

§ 17 d-e og legge frem forslag om endringer som senker terskelen for overvåkning av mulige terrorister.

4. Komiteens tilråding

Komiteen viser til sine merknader og til proposisjonen, og rår Stortinget til å gjøre følgende

vedtak:

A

Vedtak 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:

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.

Utenfor domstolens ordinære kontortid fremsettes begjæring om utlevering for Oslo tingrett etter nærmere bestemmelser gitt av departementet.

§ 210 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 femte 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:

Overskriften til § 2-7 skal lyde:

§ 2-7 *Kommunikasjonsvern m.v. Plikt till å slette data*

§ 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 § 2-7 a 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 § 2-7 a skal lyde:

§ 2-7 a. *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 6 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 gi forskift om at tilbyder kan kreve fremlagt politiattest fra personer som skal behandle lagringspliktige data på tilbyderens vegne. 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 av 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 kommunikasjon § 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

I lov 14. april 2000 nr. 31 om behandling av personopplysninger (personopplysningsloven) skal § 35 nytt annet ledd lyde:

Ved behandling av personopplysninger som skal lagres etter ekomloven § 2-7 a skal det vurderes om det bør stilles vilkår om kryptering. Kongen kan ved forskrift gi nærmere regler om slik kryptering.

VII

1. Loven gjelder fra den tid Kongen bestemmer. Kongen kan sette i kraft de enkelte bestemmelsene til forskjellig tid.
2. Kongen kan gi nærmere overgangsregler.

B

Stortinget ber regjeringen legge avtalen som den ligger i Innst. 275 L (2010–2011) til grunn for sitt arbeid med dette sakskomplekset.

Oslo, i transport- og kommunikasjonskomiteen, den 30. mars 2011

Knut Arild Hareide
leder

Ingjerd Schou
ordfører