telenor

Samferdselsdepartementet
Postboks 8010 Dep
0030 OSLO

Vår dato
12.04.2010

Vår referanse

Deres dato
08.01.2010

Deres referanse
09/585/HK

Vår saksbehandler

HØRING OM DATALAGRING - TELENORS HØRINGSSVAR

1 Innledning

Telenor viser til felles høringsbrev og -notat 08.01.2010 fra Samferdselsdepartementet, Justisdepartementet samt Fornyings-, administrasjons- og kirkedepartementet (heretter "departementene") om mulig innlemmelse av EUs direktiv om datalagring fra 2006 (direktiv 2006/24/EF) i EØS-avtalen, og derigjennom i norsk rett.

Nærværende brev er et samlet svar fra Telenor Norge AS og Telenor Broadcast Holding AS (heretter "Telenor"), det vil si fra Telenors samlede operative virksomhet i Norge.

Datalagringsdirektivet er omstridt både innen EU og i Norge. I sin avgjørelse om implementering av datalagringsdirektivet i norsk lov må Stortinget foreta en svært vanskelig avveining mellom i hovedsak tre motstridende hensyn:

- Effektiv kriminalitetsbekjempelse i en stadig mer digital verden
- Beskyttelse av privatlivets fred og personvern
- Konkurransen i markedet for elektronisk kommunikasjon

Norsk implementering av datalagringsdirektivet vil få betydelige konsekvenser for Telenor som ledende tilbyder av offentlige ekomtjenester til det norske markedet. Telenors høringssvar inneholder innspill og synspunkter som relaterer seg til alle tre nevnte hensyn, men dog med hovedvekt på de forhold som angår selskapet spesielt – de kommersielle og tekniske sidene ved direktivet. Vi vil imidlertid avstå fra å gjøre en samlet avveining av om innføring av et krav om innsamling og lagring av data til kriminalitetsbekjempelsesformål er et forholdsmessig tiltak sett opp mot personvernet. Vi registrerer at både Datatilsynet og Kripos, som rette fagmyndigheter på sine respektive felt, har adressert nettopp denne sentrale avveiningen i den offentlige debatten om datalagringsdirektivet, om enn de to partene har kommet til motstridende konklusjoner.

1.1 Oppsummering av høringssvaret

Telenors primære hensyn i forbindelse med datalagringshøringen er ivaretakelse av tillitsforholdet til kundene våre samt å unngå vridning av konkurransen i markedet. Med dette utgangspunkt er det Telenors *prinsipale* synspunkt, at datalagringsdirektivet *ikke* bør implementeres i norsk rett.

Etter vår vurdering legger direktivet, selv med de innskrenkende presiseringer og grensedragninger EU-Kommisjonens ekspertgruppe anbefaler, opp til en omfattende, på mange måter uklar, og til tider tilsynelatende uhensiktsmessig lagringsplikt for tilbydere av elektroniske kommunikasjonstjenester, som gjør det vanskelig å overskue de langsiktige konsekvensene av en implementering for hhv. kriminalitetsbekjempelse, personvern og konkurranse.

Datalagringsdirektivet vil pålegge Telenor å samle inn og lagre store mengder informasjon om kundenes bruk av våre tjenester som Telenor ikke har forretningsmessig behov for. Hvilke typer av data dette gjelder vil vi komme nærmere tilbake til i kapittel 2.

Telenor har registrert at enkelte aktører i debatten har fremstilt direktivets krav til lagring som om det utelukkende stilles krav om at data om elektronisk kommunikasjon *ikke slettes*, men bare tas vare på noe lenger enn i dag. Telenor vil påpeke at denne beskrivelsen ikke er dekkende for de omfattende tiltakene Telenor og andre ekomtilbydere vil måtte iverksette for teknisk å imøtekomme direktivets krav til hva som skal lagres. Direktivets spesifikasjon innebærer – også selv om vi legger en innskrenkende tolkning til grunn - at vi på flere områder vil måtte gjøre betydelige investeringer og inngrep i nettene for å legge til rette for systematisk innsamling og lagring av data, som vi altså ikke selv trenger, utelukkende med tanke på kriminalitetsbekjempelse. Å redusere direktivets praktiske konsekvenser til et spørsmål om "ikke sletting" blir derfor lite treffende.

Verken departementenes høringsnotat eller den offentlige debatten om datalagring har etter vårt syn i tilstrekkelig grad belyst hva som er alternativene til full implementering av dagens datalagringsdirektiv.

Det burde for eksempel vært vurdert om formål og intensjon med direktivet kunne vært oppnådd med mer målrettede tiltak – for eksempel ved å åpne for utvidelse av lagringstiden for data som ekomtilbydere allerede tar vare på til egne forretningsmessige formål, slik at disse data fortsatt er tilgjengelige for politiet til kriminalitetsbekjempelsesformål; også utover den tiden ekomtilbyderne selv har forretningsmessig behov for å ta vare på de aktuelle data. ISPenes sletting av IP-adresser etter tre uker (etter pålegg fra Datatilsynet) er det eksemplet Kripos selv nevner oftest og fremhever som den største barrieren for effektiv etterforskning og forebygging av kriminalitet.

I tilfelle resultatet av Stortingets behandling av datalagringssaken blir at direktivet innlemmes i EØS-avtalen, og Telenors prinsipale innstilling derved ikke imøtekommes, innholder høringssvaret også en forholdsvis utførlig beskrivelse av Telenors *subsidiære* synspunkter på *hvordan* vi mener datalagringsdirektivet mest hensiktsmessig kan implementeres i norsk rett. Det er vår klare anbefaling at en eventuell norsk implementering av EU-direktivet må legge seg på et minimum i forhold til å oppfylle direktivets bestemmelser og i tillegg bringe klarhet i blant annet *hva* som nøyaktig skal lagres, av *hvem*, *hvor* og *hvordan* dette skal skje, *hvor lenge* samt *til hvilke formål* utlevering av lagrede data skal skje.

1.1.1 Nærmere om Telenors prinsipale synspunkt: Ikke-implementering av direktivet

Internasjonale erfaringer med datalagring
Direktivet har både nasjonalt og internasjonalt vært gjenstand for en interessant debatt om personvernets stilling, menneskerettighetenes innhold og rettsstatens kvalitet. Telenor følger denne debatten med interesse.

Ennå er ikke direktivet implementert i alle EU-medlemsland, og flere nasjonale domstoler vurderer direktivet i forhold til nasjonale forfatninger og bestemmelser om personvernet. Rettsavgjørelser i både Romania og nå senest i Tyskland har vært meget kritiske i så henseende og funnet implementeringen av direktivet i strid med forfatningen. I Romania har en kommet fram til at direktivet som sådan er i strid med forfatningen, mens i Tyskland har en kommet fram til at det er selve implementeringen av direktivet i tysk rett som er i strid med forfatningen. Den norske høringsrunden vil være avsluttet før EU har avsluttet sin egen evaluering av direktivet. Denne evalueringen, som ventes avsluttet i september 2010, bør gi svar på om direktivet har fungert etter hensikten i de landene hvor direktivet har blitt implementert. Telenor mener derfor at det er tungtveiende samfunnshensyn som taler for at Stortingets behandling av spørsmålet om innføring av datalagring i Norge blir gjenstand for en grundig utredning hvor resultatene fra EUs evaluering også er med.

Kriminalitetsbekjempelse i en ny teknologisk hverdag
Datalagringsdirektivet ble til i en tid sterkt preget av terrorfrykt og var følgelig et ledd i opptrappingen av kampen mot terror. En viktig intensjon bak direktivet var blant annet å harmonisere reglene i Europa. Det er verdt å understreke at terrortrusselen var selve utgangspunktet for dette direktivet som ble til i kjølvannet av terroranslagene i New York, Madrid og London. Imidlertid har den teknologiske utvikling på mange måter løpt fra direktivet. Utbredelsen og brukervennligheten av rent internettbaserte tjenester, som faller utenfor ekomrettens definisjon av offentlig ekomtjeneste og dermed direktivets nedslagsfelt, åpner for betydelige smutthull for å kommunisere elektronisk uten at dette omfattes av noen lagringsplikt.

Selv om det for den vanlige bruker er vanskelig med dagens teknologi å unngå å legge igjen elektroniske spor, kan en med enkle grep benytte tjenester på internett uten at internettleverandøren (ISPen) logger aktiviteten, også når det gjelder for eksempel telefoni og e-post.

For eksempel kan en sende e-post via en annen e-posttjener enn den ens egen internettleverandør tilbyr. Da er det ikke mulig for internettleverandøren å hente ut informasjon som e-post brukeren sender og mottar, og leverandøren kan heller ikke vite hvilken e-posttjener brukeren har benyttet. Dersom en benytter en e-posttjener utenfor virkeområdet for lagringskravet, eller en benytter en tjeneste som ikke er underlagt lagringskrav (for eksempel en privat e-posttjener), vil de elektroniske sporene en eventuelt legger igjen, ikke nødvendigvis være tilgjengelige. En bruker kan, med den rette tekniske innsikten, sette opp sin egen e-posttjener, og således selv bestemme hva som skal lagres.

For telefoni vil bruk av tjenester som for eksempel Ventrilo og Skype gjøre det mulig å snakke sammen som ved en vanlig telefonsamtale, men uten å måtte gå via leverandører som omfattes av lagringskravet. Dette er løsninger det er svært enkelt å ta i bruk og benytte, også for folk uten særlig teknisk kompetanse. Utbyggingen av mobilt bredbånd og tilgjengeliggjøring av blant annet Skype på mobiltelefon betyr at disse mulighetene til å omgå lagringspliktige tjenester blir stadig større.

En stor andel av internett-abonnementene benyttes av mer enn en person og svært mange norske husstander har trådløse nett. Selv om en abonnent sikrer sitt trådløse nett, er mange av de trådløse løsningene trivielle å bryte seg inn på. Ved å laste ned programmer fra nettet kan dette gjøres på få minutter. Faren for at dataene som utleveres ikke er korrekte, eller retter mistanken mot feil person, er derfor reell.

Det må antas at mange organiserte kriminelle miljøer – både i Norge og internasjonalt – har den kunnskapen og kompetansen i sitt miljø som trengs for for eksempel å sette opp løsninger med tanke på omgåelse av lagringskravet, ta i bruk ikke-offentlige ekomtjenester som ikke omfattes av lagringskrav, eller benytte seg av usikrede – eventuelt bryte seg inn i sikrede - trådløse nett. Dette betyr sannsynligvis at de som først og fremst vil få lagret sin elektroniske kommunikasjon i henhold til datalagringsdirektivet primært vil være små, dårlig- eller ikke-organiserte grupper av kriminelle, samt alminnelige brukere uten kriminelle hensikter.

Telenor har forståelse for politiets behov for å kunne ta i bruk elektroniske spor i sin etterforskning, men en innføring av datalagringsdirektivet åpner for så mange smutthull at det er betimelig å stille spørsmålstegn ved hvor effektivt et slikt tiltak i realiteten vil være i forhold til forebygging og bekjempelse av den typen organisert kriminalitet som er formålet for lagringsplikten.

Forholdet til privatlivets fred og personvernet
For Telenor er personvernet både en grunnleggende samfunnsverdi og en viktig premiss for vår forretningsvirksomhet. Det vil være skadelig for vår virksomhet dersom våre tjenester oppfattes å utfordre personvernet.

Telenor ønsker ikke å lagre mer informasjon om kundenes data- og telefonbruk enn det vi trenger for å kunne oppfylle vår kontrakt med hver enkelt kunde. Dette handler om grunnleggende respekt for en kontraktspart. Våre kunder skal kunne stole på at den informasjonen vi har om hver enkelt behandles fortrolig. Utviklingen går i retning av stadig mer kundetilpassede tjenester skreddersydd den enkelte kundes særlige behov og bruksmønster i forhold til elektronisk kommunikasjon. For å kunne tilby markedet nye tjenester er det en forutsetning at kundene har tillit til den som sitter på store mengder informasjon om hver enkelt kundes bruk av elektroniske kommunikasjonstjenester. Dette tillitsforholdet blir følgelig viktigere i takt med utviklingen av nye tjenester.

I dag lagrer Telenor trafikkdata som har betydning for fakturering, i tre måneder for kunder med månedsfakturering og i fem måneder for kunder med kvartalsfakturering i henhold til konsesjon fra Datatilsynet. I unntakstilfeller hvor det er tvist om betalingen eller betaling av andre grunner ikke har funnet sted, lagres dataene inntil tvisten er løst eller betaling er mottatt. I henhold til en bransjeavtale med Datatilsynet samt pålegg Datatilsynet har gitt i henhold til dette, skal data om IP-adresser slettes etter tre uker. Data lagres således for legitime, kommersielle forhold og ivaretar behovet i forhold til hver enkelt kunde.

Det går imidlertid et skarpt skille mellom å lagre informasjon for å kunne levere og fakturere de tjenestene kundene benytter og det å bli pålagt å samle inn og lagre informasjon som utelukkende skal benyttes til andre formål, i dette tilfellet kriminalitetsbekjempelse. Et sentralt spørsmål i denne sammenheng er i hvor stor grad aktører som Telenor og andre tilbydere av elektronisk kommunikasjon skal ha en sentral rolle i å samle inn data for politiets kontroll av kundene. Telenor har forståelse for at politiet har behov for elektroniske spor i etterforskningsøyemed, men fremfor å innføre datalagringsdirektivet mener vi at man bør se om det i stedet kan gjøres endringer innenfor dagens regelverk.

Hensynet til konkurransen i markedet for elektronisk kommunikasjon
Departementene påpeker at det i noen tilfeller kan være usikkert om enkelte tilbydere eller andre aktører innenfor området vil være omfattet av lagringsplikten. Telenor mener det er svært uheldig at

direktivets virkeområde er så uklart definert. Datalagringsdirektivets nedslagsfelt er tilbydere av offentlige ekomtjenester som for eksempel fast-, bredbånds- eller mobiltelefoni. Tilbydere av tilsvarende tjenester levert over en peer-to-peer IP-basert tjeneste som for eksempel Skype, er derimot ikke nødvendigvis er inkludert. Direktivet er med andre ord ikke konkurransenøytralt, og gir ikke ønsket forutberegnelighet og like konkurransevilkår for aktørene.

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

Per i dag er det dessuten slik at tilbydere av offentlig bredbåndstelefoni til det norske markedet kan etablere hele eller deler av tjenesteproduksjonen utenfor EØS-området og derved slippe å betale merverdiavgift til Norge. Telenor har som kjent tatt til orde for at slike myndighetsskapte konkurransefordeler for enkeltaktører bør fjernes, uten at vi har nådd frem med dette synspunktet. Dersom norske myndigheter og domstoler i tillegg måtte legge til grunn en tolkning av datalagringsdirektivet som åpner for at de samme aktørene i praksis går fri av alle lagringskrav og derved vrir konkurransebildet ytterligere, blir konkurransesitasjonen ytterligere forverret for aktører som driver sin virksomhet i Norge.

Telenor har begrensede ressurser til rådighet for IS/IT-utvikling og oppfølgning av regulatoriske pålegg. Allerede i dag er bransjen underlagt en lang rekke sektorspesifikke krav. Telenor ønsker selvsagt at våre ressursprioriteringer i størst mulig grad er forretningsmessig begrunnet. Selv med full statlig finansiering av kostnadene ved implementering av datalagringsdirektivet, vil tilbyderne likevel måtte bruke betydelige mengder av både tid og ressurser på å følge opp kravet.

Også av hensynet til konkurransesituasjonen mener Telenor at datalagringsdirektivet ikke bør implementeres i norsk rett.

1.1.2 Telenors subsidiære synspunkter i tilfelle direktivet implementeres i norsk rett

Punktene under oppsummerer kortfattet Telenors vesentligste innspill gitt at det innføres krav om datalagring i henhold til EUs direktiv i Norge.

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

Ikke alt som er foreslått lagret vil være data som er enkelt tilgjengelig for ekomtilbyderne for lagring til kriminalitetsbekjempelsesformål. Dette gjelder i særlig grad data som i utgangspunktet kun finnes tilgjengelig i begrensede tidsrom i systemene, for eksempel data som kun behandles for operative formål og dermed på et annet nivå enn støttesystemene normalt lagrer data. I tillegg er det

på flere områder uklart hva som omfattes av lagringsplikten, og dette gjør det vanskelig å forutsi om det er mulig og økonomisk forsvarlig å fremskaffe og lagre dataene.

Telenor forutsetter at norske myndigheters krav til lagring i størst mulig grad avgrenses til informasjon tilbyderne allerede har lett tilgjengelig, eller som kan fremskaffes uten store problemer. Vi forutsetter videre at direktivkrav, som fremstår som uforholdsmessige og ubegrunnede hensett til formålet, ikke implementeres i norsk rett.

Telenor vil gjøre oppmerksom på at kvaliteten på de enorme datamengder som i henhold til direktivet skal lagres kan være varierende og er fastsatt ut fra våre forretningsmessige behov og hensynet til kostnadseffektiv produksjon. Data som for eksempel kun anvendes til feilsøkingsformål vil typisk holde en lavere kvalitet enn data som legges til grunn for fakturering av kunder. Telenor forutsetter at det ikke må iverksettes tiltak for å endre på dette.

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

Hvis for eksempel web-baserte tjenester ikke pålegges de samme reglene for lagring, er det ikke usannsynlig at kunder, også de som ikke har kriminelle hensikter, ønsker å flytte til de tjenestene/leverandørene som ikke er pålagt å lagre logger om databruken.

Telenor støtter departementenes forslag om at det i forskrift eller enkeltvedtak kan pålegges en lagringsplikt overfor andre enn de som faller inn under tilbyderbegrepet, dersom det er nødvendig for å oppnå formålet med bestemmelsene om lagringsplikt.

Lagringssted
Telenor støtter departementenes forslag om at den enkelte tilbyder selv velger lagringsløsning.

Vi støtter også at det skal være tillatt å lagre innen EØS.

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

Krav til lagring og utlevering av lagrede data
For å sikre forutberegnelighet for tilbyderne bør krav til utlevering spesifiseres nærmere i forskriftsform. Telenor vil i den forbindelse gjøre oppmerksom på at krav om korte leveringsfrister for utlevering og høy detaljeringsgrad i rapporter til myndighetene vil kunne være svært kostnadsdrivende.

Telenor støtter at Norge følger europeiske standarder, og vil også oppfordre til at myndighetene sikrer at alle norske tilbydere stilles overfor harmoniserte/standardiserte krav til utlevering.

Politiets og andres tilgang til data
Telenor støtter i utgangspunktet foreslått "terskelhevning" for utlevering av data som langt på vei synes å oppfylle direktivets krav om utlevering bare i "særlige saker", spesielt når en tar i betraktning at bakgrunnen for direktivet var bekjempelse av terrorhandlinger.

Telenor hadde dog gjerne sett at det hadde vært lagt opp til at domstolene på hensiktsmessig måte hadde kunnet benytte PT som et ekspertorgan i disse sakene, for eksempel ved at spørsmålet om fritak fra taushetsplikten fortsatt skulle forelegges PT.

Dersom andre myndigheter skal få tilgang til data, bør det som et absolutt minimum stilles de samme kravene til dem som til politiet for utlevering av informasjon.

For ordens skyld vil vi peke på at det konkrete lovforslaget verken oppfyller intensjonen om at utlevering til politiet kun kan skje via domstolene eller intensjonen om at det kun er data som er lagret i henhold til lagringsplikten som kan utleveres politiet.

Kompensasjon for negative konsekvenser
For alle tilbydere av lagringspliktige ekomtjenester vil det være store konsekvenser forbundet med å implementere og etterleve datalagringsdirektivets krav i form av betydelige IS/IT-relaterte kostnader direkte relatert til teknisk implementering av lagringskravene og tilrettelegging for innsamling og uthentning av data. I tillegg vil direktivet også få en rekke mer indirekte og vanskelig kvantifiserbare negative konsekvenser for ekomtilbydere som Telenor.

Telenor mener at merkostnadene som datalagringsplikten påfører ekomtilbyderne bør dekkes av myndighetene/staten i og med at kriminalitetsbekjempelse er et samfunnsanliggende. Full kostnadsdekning av tilbydernes merkostnader som følge av pålegg om datalagring vil også være nødvendig for å begrense de konkurransevridende virkninger av et slikt pålegg.

I høringssvarets kapitel 2 til 5 vil Telenor først og fremst utdype våre subsidiære synspunkter og innspill, det vil si gitt at Stortinget beslutter å innlemme datalagringsdirektivet i EØS-avtalen, og Telenor - i likhet med bransjen for øvrig - vil måtte implementere et etterfølgende norsk regelverk på området. Kapitlene vil imidlertid også i betydelig grad inneholde observasjoner til støtte for vårt prinsipale synspunkt, nemlig at direktivet ikke bør implementeres i norsk rett.

2 Teknisk implementering av datalagringsdirektivet

2.1 Manglende klarhet i det foreslåtte regelverket
Som tidligere beskrevet, er Telenors primære hensyn forholdet til kundene og konkurransen i markedet. Blant annet av denne grunn er vi bekymret for en innføring av direktivet i norsk rett. Telenor mener derfor at dersom direktivet blir innlemmet i norsk rett, må dette gjennomføres på en slik måte at en unngår konkurransevridning mellom ulike teknologier og at en allmenn skepsis knyttet til lagring fører til begrensninger i utvikling og bruk av nye tjenester. Telenor mener at det foreliggende høringsnotat ikke gir en tilstrekkelig og betryggende gjennomgang av sakskomplekset generelt og de tekniske konsekvenser spesielt. Særskilt gjelder dette uklarheter i hva som omfattes av lagringsplikten.

Basert på det nåværende underlagsmaterialet, er det vanskelig for oss å overskue de totale konsekvensene ved en eventuell implementering av direktivet. Det foreliggende lovforslag gir ikke tilstrekkelige avklaringer. Vi forutsetter derfor at det utarbeides et mer detaljert underliggende forskriftsregelverk dersom krav til datalagring gjennomføres i norsk rett. Uten mer detaljerte forskrifter vil lovpålegget om lagring bli stående som uklart og potensielt altomfattende, og den enkelte tilbyder vil måtte basere seg på ulike tolkninger fra bransjen og tilsynsmyndigheter for å kunne implementere lovverket. Dette vil i så fall være en vanskelig situasjon for tilbyderne med tanke på de store tilpasninger i nettet og investeringer som vil være nødvendig for å kunne implementere direktivet.

Telenor vil i de følgende kapitler gi noen kommentarer og eksempler på områder der høringsnotatet ikke gir tilstrekkelige vurderinger og avklaringer eller er uklart i sine krav.

2.2 Hva skal lagres – og kan vi lagre det?

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

Denne problemstillingen vil kunne forsterkes ved utvikling av nye tjenester. Nye tjenester som i dag eller på kort sikt ikke har stort omfang og ikke er omfattet av krav til lagring av data, vil kunne få et mye større omfang i fremtiden. Dermed øker behovet for lagring av data også for disse tjenestene. Anvendelse av de foreslåtte krav til lagring i en ny teknologisk hverdag vil i verste fall kunne føre til en sterk begrensning i hvilke tjenester som vil kunne tilbys i markedet. Det er derfor viktig at kravene til lagring av data ikke utformes på en slik måte at det blir en hemsko for utvikling og anvendelse av nye tjenester.

Direktivets beskrivelse av hvordan en skal forholde seg til abonnentopplysninger, er meget uklar. Direktivet og høringsnotatet beskriver at både A-, B- og C-nummer skal lagres, men ikke av hvilken tilbyder. Dersom en samtale berører abonnenter tilknyttet forskjellige tjenestetilbydere (uavhengig av om anropet går i forskjellige eller samme nett), vil ikke alle tjenestetilbydere i utgangspunktet ha informasjon om alle involverte abonnenter. Det er Telenor sin oppfatning at hver tjenestetilbyder kun bør ha abonnentopplysninger om sine egne kunder, og at det ikke bør være et krav til enhver tjenestetilbyder å sørge for lagring av alle abonnentopplysninger knyttet til en samtale. Disse opplysningene må politiet innhente hos den enkelte berørte tjenestetilbyder selv om dette vil føre til et mer omfattende sammenstillingsarbeid for politiet. Det vil være en stor sikkerhetsmessig utfordring dersom alle tjenestetilbydere skal ha tilgang til alle abonnentdatabaser. I tillegg må tjenestetilbyderen da ha full historisk oversikt over hvem som har vært eier, bruker og betaler av abonnementet i perioden for søket.

Direktivet og høringsnotatet forutsetter at mislykkede oppringninger og mislykkede påkoplinger skal omfattes av lagringsplikten (ref. høringsnotatet kapittel 4.4.6). Når det gjelder mislykkede oppringninger (oppringingsforsøk uten svar fra B-abonnent), blir ikke informasjon om disse lagret i dag. Bakgrunnen er delvis at en Telenor ikke har behov for disse dataene fordi slike samtaleforsøk ikke faktureres. Hovedgrunnen er imidlertid at omfanget av datavolumet som da må overføres i nettet, er så stort at det ikke er kapasitet nok til dette i dag. Kravet til lagring av mislykkede

oppringninger vil derfor generere en teknisk utfordring i nettet som vil kunne føre til et behov for utvidelse av kapasiteten i nettet.

Det er uklart for Telenor hva som menes med "mislykkede påkoblinger". Feilede forsøk på oppkobling mot internett burde bety svært lite. For eksempel kan det være tilfeller der en brukers maskin gjør oppkoplingsforsøk mot internett uten at brukeren er hjemme. Med utbredelsen av xDSL og bredbånd av forskjellige typer, er det ikke unormalt at brukere er koplet opp mer eller mindre konstant og at maskinen eller modemet sørger for å holde forbindelsen oppe selv om brukeren ikke er hjemme. Ofte vil også en maskin forsøke å opprette en forbindelse på egenhånd dersom linjen brytes, uten at brukeren behøver å gjøre noe. Data om slike oppkoplinger vil overhode ikke si noe om brukers lokasjon eller dennes forsøk på å kommunisere med andre.

Det bør også klargjøres hvorvidt informasjon om mislykkede sendinger av e-post skal lagres og hva som regnes som en mislykket sending. Det finnes flere måter å tolke "mislykket sending" på. Det kan for eksempel være at e-posttjeneren aldri godtar e-posten, eller at e-posten er forsøkt sendt til en ikke-eksisterende adresse, eller at den blir stanset av et spam-filter og aldri når brukeren. Det kan imidlertid være vanskelig å skille ut data om påkoblingsforsøk eller sending av e-post der forsøket mislyktes. For e-post er ikke dette nødvendigvis synlig ut fra loggene, og e-posttjeneren kan ikke nødvendigvis identifisere dette, heller ikke i de tilfellene der e-posten aldri forsøkes levert til mottakers e-postkasse. For eksempel kan mottakers e-posttjener vurdere e-posten som en sannsynlig spam, og slette e-posten uten at den forsøkes levert til mottaker. I slike tilfeller har ikke avsenders e-posttjener mulighet til å registrere at e-posten ikke ble forsøkt levert, og sendingen vil fortsatt logges.

Tilbydere av e-posttjenester vil ikke nødvendigvis ha tilgang til informasjonen som i følge høringsnotat skal logges, på tross av at informasjonen teknisk sett ligger lagret i tilbydernes systemer. Når en e-post sendes fra avsender, vil avsenders e-posttjener kunne logge IP-adressen til avsender. E-posttjeneren vil også normalt legge ved teknisk informasjon om når e-posten er mottatt av e-posttjeneren, hvor den er mottatt fra, med mer. Dette kan sammenlignes med et poststempel, der alle e-posttjenere underveis fra avsender til mottaker setter på sitt stempel. Dette er imidlertid informasjon som lagres inne i selve e-posten, sett fra e-posttjenerens side. Det betyr at for å hente ut denne informasjonen må en gjøre det samme som om en ønsket å hente ut selve innholdet som avsenderen har sendt. E-posttjeneren verken behandler eller tar hensyn til denne informasjonen. Det skal også nevnes at en normalt, ved sending av e-post, ikke omtaler dette som å logge av og på en e-posttjener.

For bredbåndstelefoni og internettaksess, er det foreslått at det skal lagres "informasjon som identifiserer kommunikasjonsutstyr eller kommunikasjonsanlegg" (ref. høringsnotatet kapittel 4.4.3 og 4.4.4). Det er uklart hva dette innebærer. Dersom det for bredbåndstelefoni siktes til lagring av MAC-adresse, skal det nevnes at en MAC-adresse veldig enkelt kan forfalskes. Det finnes programmer på internett som gjør dette, og en kan selv gå inn og konfigurere MAC-adressen med enkle håndgrep på egne maskiner. Dersom det siktes til noe annet, bør dette utdypes nærmere.

2.3 Hvem skal lagre?

Dersom datalagringsdirektivet blir innlemmet i norsk lovgivning, støtter Telenor forslaget om at det i forskrifts form eller gjennom enkeltvedtak kan pålegges en lagringsplikt overfor andre enn de som faller inn under ekomrettens tilbyderbegrep, dersom det er nødvendig for å oppnå formålet med bestemmelsene om lagringsplikt.

I høringsnotatet nevnes eksplisitt at følgende alminnelig forekommende typer av tjenestetilbydere, som faller utenfor ekomrettens definisjon av *offentlig* tilbyder, ikke vil bli omfattet av et krav om datalagring: Lokale nettverk drevet av bedrifter, sykehus, hoteller, private borettslag og andre som utelukkende stiller sine kommunikasjonstjenester til rådighet for lukkede brukergrupper eller ansatte. Bruk av elektroniske kommunikasjonstjenester tilbudt av slike ikke-offentlige aktører, vil utgjøre opplagte og i mange tilfeller lett tilgjengelige smutthull for brukere med kriminelle hensikter.

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

For bredbåndstelefoni vil kravet til hvilken tilbyder som skal lagre data, være avhengig av løsningen som benyttes for å realisere tjenesten. For tjenester som benytter liknende peer-to-peer baserte teknologier som Skype, vil for eksempel i utgangspunktet de påkrevde data ikke kunne kreves lagret.

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

Telenor har en web-basert e-postleser tilgjengelig for sine kunder. Det virker svært kunstig dersom Telenor ikke blir pålagt å lagre data om de e-poster som sendes og mottas via dette grensesnittet, men pålegges å lagre data om e-poster som sendes via e-postprogrammer på brukernes egne maskiner. E-posten går inn til samme e-posttjener hos Telenor og håndteres på nøyaktig samme måte etter at den er sendt. Den eneste forskjellen er grensesnittet en benytter for å sende e-posten.

Det samme argumentet kan benyttes om andre web-baserte tjenester. Dersom det først skal innføres lagringsplikt, må en se på tjenestene som ytes, ikke det formatet tjenesten presenteres i. Det må også tas høyde for at tjenestene også i fremtiden vil endre seg, og det er sannsynlig at grensene mellom de forskjellige tjenestene og teknologiene vil flyttes, fjernes eller endres på annen måte. Slik forskjellsbehandling av teknologier og løsninger med hensyn på krav til lagring av data, vil både kunne virke konkurransevridende og hemmende på utvikling av ny teknologi og nye løsninger for å gi kundene bedre tjenester. Desentraliserte tjenester, det vil si tjenester der kommunikasjonen ikke er avhengig av en sentral database, tjener eller lignende, for eksempel der kommunikasjonen foregår direkte mellom to PCer (peer-to-peer), blir stadig mer populære, og på tross av mye negativ omtale i forbindelse med for eksempel piratkopiering, har dette også mange positive sider. Blant annet vil slike tjenester hjelpe til med å begrense belastning på tjenestene, og de vil være mer robuste i forhold til utfall og nedetid. Seriøse bedrifter, for eksempel NRK Beta, BBC og Blizzard som leverer nettspillet World of Warcraft, benytter slik teknologi for å forbedre sine tjenester. Det er derfor viktig at et lagringskrav ikke hemmer innovasjon og utviklingen av nye tjenester.

2.4 Lagringssted – la tilbyderne bestemme

Telenor støtter departementenes forslag om at det bør være opp til den enkelte tilbyder å velge hvordan lagring av data skal foregå, samt hva slags løsning som skal benyttes. De forskjellige tilbydere benytter svært forskjellige systemer, og det kan bli vanskelig å finne en felles løsning for alle.

En felles, sentral database vil fort bli kostbar. Det er store mengder data som da må overføres til denne databasen, selv med vaskede data. Det vil kreve stor kapasitet både for å konvertere dataene og for å overføre dem videre til databasen. Dataoverføringen vil i dette tilfelle kreve stor båndbredde. I tillegg vil enhver endring av loggene ifm vasking eller konvertering kunne føre til feil. Dersom en skal konvertere dataene til et annet format er det ikke sikkert at det finnes ferdige programmer for dette. Da må dette lages. Ethvert program kan også inneholde feil som gjør at konverteringen til et annet format feiler. Den minst dramatiske konsekvensen av dette vil være at loggene ikke er tilgjengelige. Men det er også muligheter for at en kan få feil som kan føre til at en får ut feilaktige data, som fort kan få store konsekvenser dersom det for eksempel ender med at feilaktig informasjon om en abonnent blir utlevere til politiet.

En sentral løsning vil også innebære at en får mindre kontroll over hvem som henter ut data. I tillegg blir det ett enkelt sted som kriminelle kan konsentrere angrep mot. En enkelt sentral database vil være mer sårbart for angrep enn de vanlige driftssystemene til en tilfeldig tilbyder; ikke fordi sikkerheten vil være dårligere, men fordi en slik database vil være mer attraktivt som mål. Konsekvensene av at sikkerheten i en slik sentral database kompromitteres vil også være langt større enn dersom sikkerheten hos en enkelt tilbyder kompromitteres, blant annet fordi de fleste tilbydere har separate logger for SMS, mobilsamtaler, bredbåndstelefoni, internettoppkoblinger og e-post. Med andre ord, dersom en har en sentral database, vil en sannsynligvis kunne få tilgang til alt dersom en klarer å bryte seg inn. Lagres informasjonen lokalt, vil en ha tilgang til informasjon fra det enkelte systemet en kompromitterer, for eksempel hvem som har sendt e-post, men ikke automatisk også logger som viser SMS-sendinger, mobilsamtaler eller oppkobling til internett.

På bakgrunn av ovenstående, er Telenor tilfreds med at departementene ikke går inn for sentral lagring, men foreslår at tilbyderne selv kan velge lagringsløsning.

2.5 Lagringstid – kortest mulig og lik for alle typer teknologier

Som beskrevet innledningsvis, er det Telenors prinsipale synspunkt at datalagringsdirektivet ikke bør innføres i norsk rett. Jo lenger vi eventuelt vil måtte lagre personopplysninger i henhold til datalagringsdirektivet, jo større vil inngrepet i våre kunders private sfære være. Følgelig ønsker Telenor, dersom direktivet likevel blir innført i Norge, kortest mulig lagringstid – altså maksimalt 6 måneder lagring av opplysningene.

Det bør stilles samme krav til lagringstid for alle typer teknologier. Hvorvidt en benytter bredbåndstelefoni, mobiltelefon eller fasttelefon bør ikke avgjøre hvor langt tilbake i tid politiet kan spore en samtale. Det kan fort påvirke konkurranseevnen til de forskjellige tilbyderne. Dersom for eksempel kravet til lagring av bredbåndstelefoni er kortere enn for fastnettelefoni, vil dette kunne føre til at kunder velger bredbåndstelefoni fremfor fastnettelefoni, noe som igjen vil få konsekvenser for tilbyderne av de forskjellige tjenestene.

2.6 Krav til lagring og utlevering av lagrede data – kravene må balanseres

Direktivet sier svært lite konkret med hensyn til leveransetid og krav til kvalitet ved overføring av data til politiet. Det ser ut til at det legges opp til en diskusjon/avklaring mellom tjenestetilbyderne og myndighetene (her representert ved politiet) i etterkant av en eventuell innføring av direktivet for å bli enige om leveransedetaljer. Eventuelle krav på dette området vil, etter Telenor sin oppfatning, ha stor betydning for hva slags lagrings- og overføringsløsninger som kan velges og kostnadsnivået for dette. Telenor vil derfor oppfordre departementene til å legge føringer på kravene på dette området slik at kravene balanserer mellom politiets rimelige behov og tilbydernes mulighet for å håndtere dette både teknisk og administrativt samt at kravene blir økonomisk forsvarlige.

Når det gjelder bruk av de ikke-bindende ETSI-standarderne for lagring og utlevering av data, mener Telenor at myndighetene bør sørge for at standardene ligger som et fundament for hvordan datalagring skal gjennomføres i Norge. Standardene bør om nødvendig tilpasses forholdene i Norge. Bruk av ETSI-standardene vil kunne føre til at vi kan få positive synergieffekter fra andre land som allerede benytter standardene.

3 Utlevering av lagrede data

3.1 Myndighetstilsyn med lagring og utlevering

Dersom datalagringsdirektivet skal gjennomføres i norsk rett, støtter Telenor departementenes forslag i pkt. 4.10 om at dagens tilsynsordning med et delt ansvar mellom Post- og teletilsynet og Datatilsynet opprettholdes. Dette må gjelde tilsyn både med den pålagte lagring og med utlevering av pålagt lagrede data. Telenor støtter også departementenes forslag om å be tilsynene avklare grensedragningen mellom enhetenes utøvelse av tilsyn innenfor dette saksområdet.

3.2 Statistikk

Telenor støtter fullt ut direktivets forslag i pkt. 4.11 om at det er politiets oppgave og ansvar å utarbeide statistikk over utleverte data og rapportere dette videre til Post- og teletilsynet. Dog bør dette ikke være til hinder for at ekomtilbyderne har adgang til å hente ut egne statistikker og rapporter fra eget lagringssystem for internt bruk, eksempelvis for kartlegging av ressursbruk, bemanning, investeringer, fakturering av politiet etc.

3.3 Politiets tilgang til data

Som påpekt av departementene i pkt. 1.2, fastsetter direktivet i Art. 1.1 at datalagring kun kan pålegges i forbindelse med avdekking, etterforskning og rettsforfølgning av alvorlige straffbare forhold. I henhold til direktivets Art. 4 skal utlevering bare kunne kreves i særlige saker. Direktivet krever altså at listen skal legges høyere enn hva dagens regelverk for uthenting av data forutsetter, hvor det eneste kravet i prinsippet er at det er startet etterforskning av et straffbart forhold (men hvor PT – blant annet ut fra forholdsmessighetsprinsippet i straffeprosesslovens § 170a - kan nekte fritak fra den lovbestemte taushetsplikt).

Oppfyllelse av disse skjerpede kravene for utlevering har departementene forsøkt løst ved å kreve en kvalifisert mistanke - "*skjellig grunn*" – og at mistanken skal gjelde forbrytelser som har en viss strafferamme eller av andre grunner anses særlig alvorlige.

Departementene har i sitt forslag ytterligere hevet terskelen, ved å legge opp til at det i hvert enkelt tilfelle skal være retten som tar stilling til utleveringskravet fra politiet/påtalemyndigheten.

Telenor støtter i prinsippet en slik "terskelhevning" som langt på vei synes å oppfylle direktivets krav om utlevering bare i "særlige saker", spesielt når en tar i betraktning at bakgrunnen for direktivet var bekjempelse av terrorhandlinger.

Det er imidlertid et spørsmål om denne terskelhevningen for utlevering kompenserer den økte personvernrisiko den massive datalagringen representerer. Denne økte risikoen skyldes både at det er tale om vesentlig større mengder lagrede data enn i dag og at det kan bli aktuelt med lagring hos et stort antall aktører med varierende kompetanse, erfaring og rutiner i tilknytning til lagring av slike store mengder data av til dels følsom karakter.

Telenor har oppfattet det slik at departementene har en intensjon om at de skjerpede krav i forbindelse med utlevering til politiet skal gjelde for all utlevering av informasjon som er omfattet av taushetsplikten i ekomloven § 2-9 første ledd, uavhengig av om denne informasjonen er lagret som følge av lagringsplikten eller om den er lagret til bruk for tilbyderens eget formål (fakturering og gjennomføring av tjenestene). Høringsnotatet er ikke helt klart på dette punktet, men denne forståelsen er bekreftet av Samferdselsdepartementet på et åpent seminar om datalagring.

Ovennevnte skjerpelse av dagens praksis er i utgangspunktet positiv, sett fra et personvernsynspunkt, men Telenor ser likevel at det kan ha uheldige sider. Dette er kort kommentert nedenfor under spørsmålet om de skjerpede kravene bør gjelde for utlevering av alle data.

3.4 Spesielt om domstolsbehandling som grunnlag for utlevering

Telenor støtter intensjonen bak forslaget om domstolsbehandling før utlevering til politiet, nemlig å markere at det ikke skal være kurant å få utlevert de data som er blitt lagret i henhold til lagringsplikten.

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

Post- og teletilsynet sitter med en god del kompetanse om bransjen og teknologier som benyttes. En kan imidlertid ikke forvente at den enkelte dommer nødvendigvis har den samme tekniske kunnskapen og forståelsen som er nødvendig for å kunne gjøre en grundig vurdering av et utleveringskrav. PT vil, med sin bakgrunn og sitt virkeområde, ofte være i bedre stand til å vurdere relevansen og konsekvensen ved utlevering av de dataene som politiet ber om å få tilgang til. Dette er ikke tilstrekkelig hensyntatt i høringsnotatet. Telenor hadde gjerne sett at det hadde vært lagt opp til at domstolene på hensiktsmessig måte hadde kunnet benytte PT som et ekspertorgan i disse sakene, for eksempel ved at spørsmålet om fritak fra ekomlovens taushetsplikt fortsatt skulle forelegges PT.

For ordens skyld nevnes at vi under kommentaren til de konkrete lovendringsforslag, påviser at det konkrete lovforslaget ikke oppfyller intensjonen om at utlevering til politiet kun kan skje via domstolene. Heller ikke intensjonen om at det kun er data som er lagret i henhold til lagringsplikten som kan utleveres politiet, er ivaretatt i lovforslaget.

3.5 Bør de skjerpede krav gjelde for utlevering av alle data?

Telenor forutsetter at de skjerpede krav for utlevering, herunder domstolsbehandling, ikke gjelder informasjon som er omfattet av ekomloven § 2-9 tredje ledd, slik at politiet fortsatt kan få direkte tilgang til abonnentinformasjon fra tilbyderne, uten å gå veien om domstolene.

Heller ikke i nødrettstilfeller vil de skjerpede krav gjelde. Således vil politiet, under henvisning til at det foreligger en nødrettssituasjon etter straffeloven § 47, kunne få de nødvendige data direkte fra tilbyderne på meget kort varsel, uten å gå veien om domstolene, slik tilfellet også er i dag.

Telenor ser i tillegg at det kan være en utfordring for effektiviteten av politiets arbeid at det – slik forslaget legger opp til i dag - ikke vil være adgang til å bruke ekomrelaterte elektroniske spor i etterforskningen av en rekke straffbare handlinger som ikke oppfyller de foreslåtte skjerpede krav. Dette representerer en relativt kraftig innskrenkning av den adgang til slike spor som politiet har i dag.

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

3.6 Andre myndigheters tilgang til data

Selv om direktivet overlater til de enkelte medlemsstater å avgjøre hvilke myndigheter som kan gis tilgang til de pålagt lagrede data, er det i Norge ikke naturlig å gi direkte tilgang for andre myndighetsorganer enn politi og påtalemyndighet. Telenor støtter derfor departementenes forslag om at tilgang til de lagrede data bare skal gis til politi og påtalemyndighet. Om for eksempel skatte- og avgiftsmyndigheter har behov for tilgang, vil de - som departementene påpeker – kunne anmelde det aktuelle forhold, hvoretter politiet avgjør om det er hensiktsmessig å innhente de lagrede data.

For ordens skyld gjør Telenor oppmerksom på at den adgang enkelte kontroll- og tilsynsorganer i henhold til særlovgivningen har til å innhente visse opplysninger fra ekomtilbydere, i de aller fleste tilfeller er begrenset til navn og adresse til enkeltkunder og ikke omfatter trafikkdata, sporingsdata og lignende.

At andre myndigheter også skal kunne få tilgang til lagrede data, og at kravet til utlevering kan komme til å bli lavere enn kravet for utlevering til politiet, er svært foruroligende. Eksempelvis er etterforskning av økonomisk kriminalitet ikke et formål som direktivet opprinnelig var ment å brukes til.

Dersom andre myndigheter skal få tilgang til data, bør det som et absolutt minimum stilles de samme kravene til dem som til politiet for utlevering av informasjon.

Telenor registrerer at det ikke er foreslått endring i verdipapirhandelloven § 15-3 annet ledd nr 3, hvilket tilsier at Finanstilsynet ikke behøver å gå veien om domstolene for å få utlevert trafikkdata etc. som er pålagt lagret eller som ekomtilbyderen måtte besitte av hensyn til egne behov. Det kan spørres om det er tilstrekkelig gjennomtenkt at Finanstilsynet skal ha lettere adgang til disse dataene enn politiet.

3.7 Andres tilgang til data

Telenor ønsker å understreke viktigheten av at pålagt lagrede data ikke blir tilgjengeliggjort for andre enn politi, påtalemyndighet og eventuelle andre myndighetsorganer. For eksempel må ikke innføringen av datalagringsdirektivet føre til at kommersielle aktører kan få tilgang til data, slik som identiteten til en abonnent basert på en gitt IP-adresse og et gitt tidspunkt. Om det er behov for slike data i tiknytning til en sivilrettslig tvist, bør det reguleres av tvisteloven. At data som er pålagt lagret utelukkende av hensyn til etterforskning av alvorlig kriminalitet (men som ellers av personvernmessige hensyn ville ha vært slettet), skal kunne føres som bevis i sivile saker, er på ingen måte en selvfølge.

3.8 Post- og teletilsynets rolle

Post- og teletilsynet besitter en høy kompetanse relatert til ekombransjen generelt og de elektroniske spor brukere etterlater seg, spesielt. PT vil følgelig i mange sammenhenger være bedre i stand til å vurdere relevansen og konsekvensen av politiets krav om utlevering av – ofte meget omfattende mengder - data, enn hva domstolene vil være.

Som anført ovenfor i tilknytning til domstolenes rolle, er derfor Telenor bekymret for konsekvensen av at PT fullstendig fratas sin rolle i å vurdere spørsmål om fritak fra taushetsplikten for de lagrede dataene før retten fatter sin beslutning. Det kan derfor med god grunn reises spørsmål ved om ikke PT fortsatt bør ha ansvaret for å vurdere politiets begjæring om utlevering av data opp mot den lovbestemte taushetsplikten og – eksempelvis – det straffeprosessuelle forholdsmessighetsprinsipp, slik straffeprosessloven § 118 første ledd forutsetter. Domstolen vil uansett ha en mulighet til å overprøve PTs vurdering etter § 118 annet ledd.

4 Konsekvenser for kostnader, etterspørsel, omdømme og risiko

For alle tilbydere av lagringspliktige ekomtjenester vil det være store konsekvenser forbundet med å implementere og etterleve datalagringsdirektivets krav.

Det vil opplagt være betydelige IS/IT-relaterte kostnader direkte relatert til teknisk implementering av lagringskravene og tilrettelegging for innsamling og uthentning av data under. I tillegg vil direktivet også få en rekke mer indirekte og vanskelig kvantifiserbare negative konsekvenser for ekomtilbydere som Telenor, blant annet i form av konkurransevridning, omdømmerisiko og tilleggskrav til nye tjenester.

4.1 Kostnader forbundet med innføring av datalagringsplikt

Telenor har i høringsperioden forsøkt å oppstille et grovt estimat av IS/IT relaterte kostnader basert på tilgjengelige opplysninger i datalagringsdirektivet, departementenes høringsnotat, anbefalinger fra EUs ekspertgruppe samt erfaringer fra land som har implementert direktivet. Vi har imidlertid konkludert med at det - på det foreliggende grunnlag - fremstår som særdeles uklart hva som vil bli lagringskravene i en mulig fremtidig norsk implementering av direktivet. I erkjennelse av at regnestykkets forutsetninger er både svært usikre og uklare, har vi valgt å *ikke* antyde et tall for estimerte kostnader forbundet med Telenors eventuelle implementering av datalagringskravene. Av samme grunn har vi også valgt å avstå fra å kommentere på Teleplans økonomiske konsekvensutredninger.

Telenor vil likevel peke på de vesentlige kostnadsdriverne som vil påvirke kostnadene av lagringsplikte ekomtjenester:

- **Lagringskravets omfang**:
  Kostnadene ved å legge til rette for innsamling og lagring av data som i dag ikke lagres eller er tilgjengelige vil kunne være omfattende.
- **Krav om logisk atskillelse**:
  Krav om at data som skal lagres i henhold til direktivet må holdes logisk adskilt fra andre data ekomtilbyderne lagrer, innebærer i praksis at det må utvikles et nytt system for datalagringen. Dette betyr at også de tilbyderne som logger data i dag og som har en infrastruktur og et nettverk som støtter lagring av data, likevel vil måtte investere i nye systemer, nye lisenser, nytt utstyr, mer lagringsplass med videre.
- **Lagringsperiode**:
  Kostnadene vil øke desto lenge man skal lagre data, dette på grunn av at datamengden øker. I tillegg vil det påløpe større kostnader og høyere risiko fordi kapasitet og hastighet må økes for å kunne gjennomføre sikkerhetskopiering innen rimelig tid. Kostnadene vil inntil en viss grad øke lineært i forhold til økt lagringstid, men når man kommer til et kritisk høyt nivå i datamengde vil en større investering i kapasitet måtte gjøres. Det samme vil være tilfelle dersom datamengden øker på grunn av økt trafikk, men denne utviklingen vil være mye vanskeligere å forutsi.
- **Krav til utlevering**:
  Dersom man pålegger operatørene korte leveringsfrister vil krav til automatisering og bemanning, og dermed også kostnadene, øke i forhold til systemstøtte.
- **Detaljeringsgrad**:
  Det vil være svært kostnadsdrivende for operatørene dersom det blir avkrevd høy detaljeringsgrad i rapporter til myndighetene. Hvis man for eksempel skal hente ut rapporter med navn, adresse mv. pr. avsender og mottaker, vil dette være svært kapasitetskrevende
- **Krav til redundans/reserveløsninger**:
  Dersom det blir satt høye SLA-krav i forhold til feil- og katastrofesituasjoner vil det være nødvendig å etablere redundante systemer, alternativt reserveløsninger. Dette vil være svært kostnadsdrivende, da alt må dubleres og ekstra teknologi må innføres for å håndtere dette.
- **Datakvalitet**:
  Kvaliteten på data som ikke har vært ansett som nødvendige for fakturering, har ikke nødvendigvis samme kvalitet som faktureringsdata. I og med at slike data normalt benyttes i forbindelse med drift, vedlikehold og feilsøking, er behovet for nøyaktighet her ikke det samme som for fakturering. Dette betyr blant annet at man ikke har samme krav til at alt blir logget, eller at tidspunkt er like nøyaktig som i de deler av infrastrukturen som benyttes til eksempelvis taksering. Utbedring av dette kan kreve kostbare endringer av systemer, eller være svært vanskelig å få til i praksis.

Telenor, har begrensede ressurser til rådighet for IS/IT-utvikling og oppfølgning av regulatoriske pålegg. Allerede i dag er bransjen underlagt en lang rekke sektorspesifikke krav. Selv om myndighetene bestemmer seg for full statlig finansiering av kostnadene ved implementering av datalagringsdirektivet, vil tilbyderne likevel måtte bruke betydelig både tid og ressurser på å følge opp kravet.

4.2 Kompensasjon for negative konsekvenser?

Høringsnotatet omtaler ganske overfladisk hvordan datalagringsdirektivets eventuelle implementering i norsk rett forventes å påvirke konkurransesituasjonen i ekomsektoren, og nevner så vidt risikoen for at økt datalagring vil kunne medføre at kundene blir mer tilbakeholdne med å anvende elektronisk kommunikasjon.

Det er på denne bakgrunn ikke overraskende at spørsmålet om kompensasjon av tilbyderne av lagringspliktige ekomtjenester utelukkende fokuserer på IS/IT og personalrelaterte kostnader ved implementering av direktivet. I lys av de potensielt vidtrekkende negative konsekvenser for tilbyderne som er påpekt over – og som går langt ut over de rent tekniske implementeringskostnadene – mener Telenor at departementenes utgangspunkt for å diskutere kompensasjon blir for snevert.

Høringsnotatet foreslår en videreføring av dagens delingsmodell hvor ekomtilbyderne har en tilretteleggingsplikt og forutsettes å dekke kostnadene til denne plikten, mens tilbydernes driftskostnader/uthentingskostnader dekkes av politiet. Notatet kan gi inntrykk av at videreføring av delingsmodellen også innebærer at kostnadsbyrdeforholdet mellom tilbyderne og politiet videreføres uendret. Dette vil på ingen måte være tilfellet.

Vi minner om Telenor per i dag ikke er pålagt en lagringsplikt, og derfor kun logger og lagrer informasjon som er nødvendig for den forretningsmessige driften. Dette er informasjon som er nødvendig for å fakturere sluttbrukere, avregne samtrafikkpartnere, foreta kapasitetsovervåkning og lignende. I og med at Telenor selv har behov for den informasjonen som eventuelt utleveres politiet, blir ikke Telenor påført nevneverdige ekstra kostnader knyttet til å lagre data som utleveres politiet. Telenor har dog per dags dato etablert særlige systemer, enheter og rutiner som i all hovedsak har til formål å håndtere forespørsler om informasjonsuthenting til politiet.
Politiets betaling for uthentning av data er en rimelig kompensasjon for de merkostnader Telenor blir påført.

I høringsnotatet foreslår departementet at data lagret i henhold til datalagringsdirektivet skal lagres logisk adskilt fra data tilbyder eventuelt vil måtte lagre til fakturerings- og kommunikasjonsformål. Videre vil omfanget av data som skal lagres øke vesentlig utover det omfang tilbyder selv har behov for å lagre. Dette – kombinert med en videreføring av gjeldende krav til ivaretakelse av personvernet – innebærer at tilbyder som en følge av datalagringsdirektivet blir påført en betydelig merkostnad for lagring av data utover det forretningsmessige hensyn tilsier, selv om tilbyderen selv ikke har noen egeninteresse av å lagre disse dataene på den foreskrevne måte. Siden det er i myndighetenes interesse at lagringen skjer, vil den naturlige følgen være at de merkostnadene som lagringsplikten påfører tilbyderne, dekkes av de samme myndighetene.

Full kostnadsdekning av tilbydernes merkostnader som følge av pålegg om datalagring vil også være den nødvendig for å begrense de konkurransevridende virkninger pålegget gir, for eksempel i forholdet mellom tradisjonelle ekom-baserte tjenestetilbydere som vil bli truffet av datalagringsdirektivet og internett-baserte tilbydere som antakelig ikke vil bli truffet i samme grad som følge av foreslåtte unntak for rent web-baserte tjenester.

5 Kommentarer til foreslåtte endringer i aktuelle lover og forskrifter

5.1 Generelt

Telenor konstaterer at ikke alle de intensjoner høringsnotatet gir uttrykk for, er hensyntatt i de foreliggende forslag til lov- og forskriftsendringer. Dette påvises nedenfor. Hvis det viser seg å være politisk flertall for implementering av direktivet i norsk rett, er det åpenbart at det kreves ytterligere lovendringer i forhold til de som er foreslått.

Høringsnotatet gir ingen klar indikasjon på at det er forutsatt ytterligere forskriftsregulering av dette området, utover den endring som er foreslått i ekomforskriften. Telenor anser dette som uheldig, da det i praksis vil oppstå en rekke tolknings- og grensedragningsspørsmål knyttet til hvilke data som skal lagres.

Ekspertgruppen etablert av EU-Kommisjonen (Commission Decision 2008/324/EC) har gitt en rekke rådgivende uttalelser knyttet til tolkningen av hva som skal lagres, for eksempel vedrørende spam, transitt, internett-telefoni og mislykkede anropsforsøk. Gruppen arbeider fortsatt med slike grensedragningsspørsmål. Disse uttalelsene vil kunne danne et godt grunnlag for forskrifter som spesifiserer nærmere hva som skal lagres og hva som ikke skal lagres, når hverken direktivteksten eller departementenes lovforslag gir noe klart svar. Av hensyn til ryddighet og forutberegnelighet vil alle interessegrupper være tjent med en slik forskriftsbasert utdypning.

5.2 Til straffeprosessloven § 210 første ledd nytt annet punktum

Telenor har ingen innvendinger mot det foreslåtte forslag i seg selv. Tvert i mot – som understreket i vår kommentar til avsnittet om utlevering til politiet - støtter vi de skjerpede krav til hvilke typer lovbrudd som vil kunne gi grunnlag for utlevering.

Imidlertid, slik forslaget er formulert, knytter det seg utelukkende til kravene som stilles ved rettens utleveringspålegg. Til tross for at det, i departementenes kommentar til dette forslaget i høringsnotatets pkt. 7 og pkt. 4.12, hevdes at denne lovendringen medfører at påtalemyndigheten ikke kan beslaglegge data i medhold av straffeprosesslovens § 205, kan ikke Telenor se at det er tilfellet. Det er følgelig behov for en bestemmelse som klart og utvetydig sier at § 205 ikke kan anvendes til beslag av data som er pålagt lagret. Hvorvidt dette bør fremgå direkte av § 205 eller tas inn annet sted i straffeprosessloven kap. 16, er ikke Telenor den rette til å bedømme.

Telenor finner grunn til spesielt å kommentere et utsagn i departementenes merknader til endring av § 210 i høringsnotatets s. 54. Det hevdes der at endringen i denne bestemmelsen i straffeprosessloven vil kunne medføre "*utlevering av alle data i et bestemt geografisk område, for eksempel et bysentrum eller en bydel*". Dette vil måtte omfatte ekstremt store datamengder, som kan representere et problem i seg selv, men dataene vil – som en følge av lagringsplikten – være tilgjengelig hos tilbyderne. En slik utlevering vil gi politiet en tilnærmet total oversikt over bevegelsene til alle personer som benytter seg av mobiltelefon, fasttelefon eller PC i det aktuelle området over den tidsperiode politiet måtte ønske og som, for de aller flestes vedkommende, overhodet ikke har gjort noe straffbart.

Telenor mener at mye taler for at å gi politiet en slik totaloversikt i forbindelse med etterforskning av et straffbart forhold, vil være i strid med proporsjonalitetsprinsippet i straffeprosesslovens § 170a og vil også kunne representere et brudd på EMK art. 8 som beskytter privatlivets fred.

5.3 Til ekomloven § 2-7 annet ledd

Telenor kan ikke forstå det annerledes enn at henvisningen i forslaget til § 2-8 første ledd skal være annet ledd.

5.4 Til ekomlovens § 2-9 nytt femte ledd

Denne bestemmelsen sikrer, slik det også er forutsatt i notatets pkt. 4.14, at den forutgående vurdering som i dag foretas av PT, nå skal foretas av retten, når utleveringen skjer som følge av rettens kjennelse. Det er imidlertid viktig å være oppmerksom på at PT fortsatt vil måtte foreta slike vurderinger når utleveringen skjer på grunnlag av beslag etter strpl. § 205, se kommentaren ovenfor til strpl. § 210 første ledd nytt annet punktum.

5.5 Til ekomforskriften § 7-2 første ledd

Departementene har foreslått en endring i ekomforskriften § 7-2 første ledd, uten at den er nærmere kommentert i høringsnotatet, til tross for at overskriften i notatets pkt. 7 sier noe annet. Den foreslåtte teksten kan gi grunnlag for misforståelser. For det første forutsetter den at trafikkdata er en undergruppe av lokaliseringsdata, hvilket neppe er helt treffende (denne svakheten finnes for øvrig også i gjeldende § 7-2 første ledd). For det andre kan ordlyden oppfattes som at det skal bevares taushet om "andre lokaliseringsdata", men ikke "trafikkdata". Det har åpenbart ikke vært meningen.

5.6 De øvrige lovforslag

Telenor har ingen kommentarer til disse forslagene.

Med hilsen
Telenor Norge AS

Harald Krohg,
Divisjonsdirektør