



Datatilsynet

MOTTATT

- 1 OKT 2010

Samferdselsdepartementet
Postboks 8010 Dep

0030 OSLO

Deres referanse
10/139- EW

Vår referanse (bes oppgitt ved svar)
10/00919-2 /HTL

Dato
28. september 2010

Høringsuttalelse - endringer i ekomloven, ekomforskriften og nummerforskriften

Det vises til høringsbrevet datert 23. juni 2010.

Høringen gjelder endringer i lovverket som regulerer elektronisk kommunikasjon. De foreslåtte endringene skal gjennomføre justeringer som er gjort i EUs regelverk på området. Videre skal forslaget imøtekomme den tekniske utviklingen og endringer i markedet.

Det vises også til e-post av 22. september hvor Datatilsynet ble innvilget utsatt frist for å komme med merknadene til lovforslaget.

Datatilsynet vil i det følgende kun bemerke forslag til endringer i regelverket som antas å ville få konsekvenser for personvernet.

Kommentarer til de foreslåtte endringer i ekomloven

Offentlig tilgang til telefoni og Internett

Datatilsynet vil understreke at offentlige betalingstelefoner og offentlige tilgangspunkter for Internett bør være en anonym tjeneste. Også i fremtiden bør det være mulig å anvende slike tjenester uten at brukeren kan identifiseres.

Definisjoner

Datatilsynet anbefaler at begrepene *bruker*, *sluttbruker* og *abonnet* gis en klar og entydig legaldefinisjon i bestemmelsen som inneholder definisjoner (forslagets § 1-5). Begrepsbruken i loven avviker fra hvordan disse betegnelse anvendes dagligtalen, og det er derfor nødvendig at begrepenes betydning klargjøres.

Angående tilbyderes anledning til å begrense sluttbrukers adgang til elektroniske kommunikasjonsnett og -tjenester (punkt 9 i høringsnotatets sammendrag)

Datatilsynet merker seg at Departementet ikke tar til orde for å pålegge tilbydere å overvåke abonnenters bruk av nettet for å avdekke ulovlig fildeling selv om tilbyderne ikke bør kunne påberope seg en ubetinget ansvarsfrihet for bruken av tjenestene som tilbys.

Datatilsynet vil bemerke at selv om tilbydere kan pålegges et medvirkningsansvar for ulovlige handlinger som tilbyder kjente eller burde ha kjent til uten at sluttbrukers mulighet til å fortsatt utføre lovbrudd ble sperret, så bør ikke tilbydere pålegges en overvåkningsplikt for å avverge at nettilgangen benyttes til lovbrudd. En slik sammenblanding av politiets og tilbydernes roller vil kunne innebære en trussel mot rettsikkerheten. Dessuten er tilgang til telefon og Internett i dag av så avgjørende betydning for den enkeltes deltakelse i samfunnet at å frata en sluttbruker, f. eks en husstand, dette godet vil kunne være et uforholdsmessig tiltak. Tilsynet stiller seg bak den foreslåtte bestemmelsen i forslagets § 2-5a.

I forslagets § 2-5 femte til syvende ledd foreslås det hvilke prosedyrer som skal gjelde for iverksetting av bruksbegrensninger ved *svindel* og *misbruk*. Av hensynet til forutberegnelighet anbefaler Datatilsynet at det i forskriften utdypes nærmere hva slags forhold det her siktes til.

Sterke personvern hensyn tilsier dessuten at det ikke vedtas prosedyrer som krever at tilbyder skal varsle den aktuelle myndighet om hvilke enkeltpersoner bruksbegrensninger knytter seg til. Det vil være en langt bedre løsning om tilbyder pålegges en plikt til å orientere berørte sluttbrukere om at tilbyders beslutning kan underlegges domstolkontroll. Tilsynet vil bemerke at høringsnotatet inneholder lite informasjon om hvordan prosedyrene skal verne sluttbrukers rettigheter og personvern i denne sammenhengen.

Geografisk lokalisering av nødanrop

I lovforslagets § 2-6 tredje ledd pålegges tilbyderne å overføre sluttbrukers navn og nødvendige opplysninger for geografisk lokalisering av nødanrop, til nødetatene. Tilsynet vil understreke at dette kravet ikke kan være til hinder for at det også skal være mulig å foreta nødanrop når det ikke finnes en registrert sluttbruker. For eksempel er det i dag mulig å kontakte nødetater fra mobiltelefoner uten simkort. Denne muligheten bør ikke avskjæres.

Datatilsynet savner en nærmere redegjørelse for dispensasjonsadgangen i den foreslåtte bestemmelsens fjerde ledd. Av høringsnotatet fremkommer det at også tilbydere av nomadisk bruk av bredbåndstelefoner plikter å tilby opprinnelsesmarkering. Tilsynet understreker det ikke kan stilles krav om nye og personverninnngripende metoder for å lokalisere slik nomadisk bruk.

Varslingsplikt ved sikkerhetsbrudd som kan true personvernet

Datatilsynet anbefaler at forholdet mellom hovedregel og unntak i den forslåtte § 2-7 snus slik at tilbyderne kun har en varslingsplikt overfor abonnent eller bruker når det er grunn til å tro at den enkelte selv vil kunne foreta grep som kan begrense konsekvensene av sikkerhetsbruddet. Tilbyderne bør imidlertid alltid ha en plikt til å orientere Datatilsynet. Tilsynet kan så etter en konkret vurdering pålegge tilbydere en plikt til å varsle brukerne når tilbyder ikke har gjort dette på eget initiativ.

Det antas at en slik plikt vil kunne bidra til å skjerpe tilbyders fokus på informasjonssikkerhet.

Taushetsplikt

I forslaget § 2-9 pålegges tilbydere og installatører taushetsplikt om innholdet i elektronisk kommunikasjon m.m. I annet ledd gis relevant myndighet adgang til å gjøre unntak fra taushetsplikten når det er nødvendig for å sikre effektiv ruting av trafikken. Datatilsynet vil på det sterkeste advare mot at det åpnes for at det gjøres unntak fra taushetsplikten. Det bør ikke være adgang til å rute ukrypterte signaler via stater som mangler lovgivning som ivaretar kravet om konfidensialitet.

Mobilregulert sone

I forslaget § 6-2a gis politiet, forsvaret og kriminalomsorgen en eksplisitt hjemmel til å opprette mobilregulerte soner, et virkemiddel som innebærer at kontakten mellom mobiltelefoner og basestasjoner i et område blokkeres, samt at identiteten til sluttbrukere som befinner seg i området kan avsløres.

Hvorvidt mobilsignaler utelukkende blokkeres (jamming) eller om det i tillegg også skjer en identifisering av mobilapparater i området er av avgjørende betydning for personvernet, og det bør derfor spesifiseres nærmere i loven hvilke av disse tiltakene som kan anvendes i de ulike sammenhenger.

Mobilregulerte soner som innebærer *identifisering* er et tiltak som kun bør anvendes når sterke sikkerhetshensyn taler for det. Det må forutsettes at politiet og kriminalomsorgen, samt Post- og teletilsynet er svært tilbakeholdne med å benytte seg av adgangen til å anvende dette virkemiddelet og gi tillatelser til opprettelse av slike soner. I premissene for forslaget er det også forutsatt det at det skal gjøres en avveining mellom samfunnets behov og personvern hensyn.

Forsvaret bør kun ha anledning til å *blokkere* mobiltrafikken i et område. Det må legges stor vekt på å minimalisere konsekvensene tiltaket vil ha på den ordinære teletrafikken. Området må altså begrenses i utstrekning og blokkeringen må ikke pågå lenger enn nødvendig.

Ved opprettelse av mobilregulerte soner må det innføres tiltak for å varsle de personer som berøres om at telefonforbindelsen vil bli blokkert og eventuelt at mobilapparater blir

identifisert. Etter tilsynets vurdering kan det bare gjøres unntak fra forhåndsvarsling ut fra politifaglige grunner. Dette bør kun skje i ekstraordinære tilfeller.

Kommentarer til de foreslåtte endringer i ekomforskriften

Tjenestene hemmelig nummer og adgang til reservasjon mot nummervisning

Datatilsynet stiller seg bak innholdet i den foreslåtte § 1-7 som pålegger tilbyderne å informere abonnenter om adgangen til å reservere seg mot nummervisning. At det gis informasjon om dette alternativet styrker den enkeltes personvern ved at sluttbruker får bedre kunnskap om hvordan man lettere kan kontrollere spredningen av egne kontaktopplysninger. For noen vil reservasjonsordninger kunne være et godt alternativ til hemmelig nummer. At operatøren pålegges å informere om dette kostnadsfrie alternativet fremmer både personvernet og forbrukervernet.

Tilsynet vil benytte anledningen til å bemerke at tilbyderne også bør pålegges en plikt til å markedsføre sluttbrukeres adgang til kostnadsfritt å reservere seg mot oppføring hos nummeropplysningstjenester. Det understrekes videre at alle som har benyttet seg av denne muligheten må kunne være trygge på at tilbydere ikke vil utlevere deres kontaktopplysninger, heller ikke til andre aktører enn virksomheter som tilbyr opplysningsvirksomhet.

Tilsynet merker seg at det i merknadene til § 6-6 om hemmelig nummer legges stor vekt på sluttbrukers tilgang til informasjon om hva tjenesten *hemmelig nummer* innebærer.

Videre foreslås det strenge krav til rutiner for å sikre at tilbyderne har med rett person å gjøre når sluttbrukere med hemmelig nummer henvender seg til tilbyder og ber om at det gjøres endringer i abonnement eller tjenester eller ber om innsyn i egne personopplysninger. Dette er av avgjørende betydning for å sikre en reell beskyttelse av identiteten til sluttbruker. Som det understrekes i merknadene er det også avgjørende for personvernet at ikke opplysninger om sluttbruker avsløres i andre tilfeller enn når tilbyder har mottatt skriftlige anmodninger fra politiet.

I den foreslåtte bestemmelsens fjerde ledd foreslås det at sluttbruker informeres skriftlig når det gjøres ulike endringer av tjenesten hemmelig nummer. Dette må avtales spesielt med eier av hemmelig nummer. Forslaget om å benytte folkeregistrert adresse i denne sammenheng må kunne fravikes fordi innehavere av hemmelig nummer også kan ha hemmelige adresseopplysninger i Folkeregisteret.

Ved portering av hemmelig nummer pålegges tilbyder å informere mottakende tilbyder om at nummeret har status som hemmelig, jf. bestemmelsen tredje ledd.

Datatilsynet anbefaler at avgivende tilbyder pålegges en tilsvarende informasjonsplikt ved portering av telefonnumre til sluttbrukere som har reservert seg mot at egne kontaktopplysninger utleveres til allmennheten, jf. gjeldende forskrifts §§ 6-2 og 6-3.

Behandling av andre lokaliseringsdata enn trafikkdata

Den foreslåtte bestemmelsen om behandling av lokaliseringsdata (§ 7-2) innebærer en forskuttering av at Datalagringsdirektivet innføres i Norge. Datatilsynets vil derfor ikke gi noen konkrete merknader til den foreslåtte bestemmelsen i denne sammenheng, men det vises til tilsynets høringsuttalelse til en eventuell implementering av direktivet i norsk rett.

Ruting av nasjonal trafikk utenfor Norges grenser

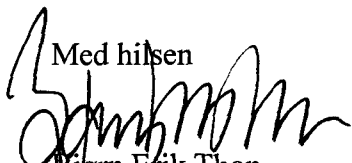
Som det fremgår av merknadene til den foreslåtte § 2-9 i loven advarer tilsynet mot at det åpnes for å rute ukryptert trafikk via land som ikke sikrer en forsvarlig håndtering av opplysningene. Risikoen ved slik ruting kan naturligvis ikke avhjelpes ved at brukerne blir informert. Tilbydere må kunne garantere for at konfidensialiteten ivaretas.

Datatilsynet er derfor av den oppfatning at ingen av de alternative løsningene som foreslås i § 7-5 kan anvendes.


Kommentarer til de foreslåtte endringer i nummerforskriften

Datatilsynet har ingen merknader til de foreslåtte endringene i nummerforskriften.

Med hilsen



Bjørn Erik Thon
direktør



Hågen T. Ljøgodt
rådgiver

Kopi: Fornyings-, administrasjons- og kirkedepartementet,
v/Statsforvaltningsavdelingen,
Pb 8004 Dep, 0030 Oslo