



➔ Samferdselsdepartementet
Postboks 8010 Dep.
0030 OSLO

Vår ref.:
1302375-2 - 008

Vår dato:
10.6.2013

Deres ref.:
12/2062

Deres dato:
26.4.2013

Saksbehandler:
Jarle Langeland

www.npt.no

Svar på høring om datalagring - forslag til regler om kostnadsfordeling, nødrettssituasjoner og taushetsbelagte data

Post- og teletilsynet (PT) viser til brev av 26.4.2013 fra Samferdselsdepartementet, der PT inviteres til å kommentere på høringsnotatet om forslag til fordeling av kostnader ved gjennomføringen av datalagringsdirektivet, uthenting av data i nødsituasjoner og utlevering av enkelte taushetsbelagte data, PUK-kode og kunderseskontro som ikke er lagringspliktig.

PT slutter seg til de vurderinger som er gjort i høringsnotatet vedrørende valg av kostnadsfordelingsmodell. PT ønsker likevel å komme med enkelte forslag til justering av modellen og de administrative ordninger som er foreslått. Videre har PT kommentarer til kapittel 3 om forslag til ny bestemmelse for politiets uthenting av data i nødsituasjoner.

PTs kommentarer til høringsnotatet:

Til kapittel 2 «Forslag til ny modell for fordeling av kostnader ved gjennomføring av datalagringsdirektivet»

Mulige konkurransevidende og etableringshindrende effekter

Etter PTs syn vil de mulige konkurransevidende og etableringshindrende effektene av lagringsforpliktelsen kunne minimeres for lagring og uthenting av data, hvor kostnadene etter forslaget skal dekkes av staten.

Imidlertid ønsker PT å påpeke at klargjøring til lagring hos den enkelte tilbyder vil medføre vesentlige investerings- og implementeringskostnader fra første kunde i en gitt tjeneste. Når systemer for lagring og klargjøring av data først er på plass, vil disse kunne betjene et visst antall kunder før det eventuelt vil måtte investeres i nye løsninger med høyere kapasitet. Det antas derfor at kostnadene per kunde for større og mer etablerte tilbydere, vil være lavere enn for mindre tilbydere- og for tilbydere i etableringsfasen.

Slike konkurransevidende effekter kan dog i noen grad kompenseres gjennom en fleksibel praktisering av refusjonsordningen som skal dekke kostnader for lagring og utlevering av data. Dette vil bli kommentert nedenfor.

Administrasjon av refusjonsordningen - sanksjonsmuligheter

PT er tilsynsmyndighet etter datalagringsforskriften, og har sanksjonsmuligheter etter forskriftens § 5-3 blant annet dersom lagringsplikten ikke blir oppfylt. Videre vil Datatilsynet kunne sanksjonere brudd på personopplysningsloven som følge av manglende sikkerhet ved lagringen.

I høringsnotatets kapittel 2.5.4, foreslås det at Politidirektoratet skal administrere refusjonsordningen, og «vil kunne holde tilbake finansiering av kostnader dersom tilbyderne ikke oppfyller de krav i lov og forskrift som følger av DLD».

Det bør klargjøres at en slik tilbakeholdelse av refusjon vil være avhengig av at ekommyndigheten har fastslått at den lagringspliktige ikke oppfyller krav til lagring i henhold til lov eller forskrift.

Oversendelse av data til felles lagringsløsning

I høringsnotatet er det lagt til grunn at refusjonsordningen skal fungere som et insentiv til at lagringspliktige tilbydere skal gå sammen om en felles lagringsløsning.

Dersom en gruppe tilbydere velger en felles lagringsløsning, oppstår spørsmålet om hvordan en skal regulere og tilrettelegge for sikker overføring av data fra tilbyders systemer til denne databasen.

For PT fremstår det som viktig at den løsning som velges for kostnadsfordeling fremmer sikkerheten for dataene gjennom hele kjeden. Dette forutsetter etter PTs oppfatning at de tilbydere som velger å inngå i en felles lagringsløsning underlegges samme krypteringsregime, og at dataene krypteres hos tilbyder før oversendelse til den felles databasen. For tilbydere som velger egne lagringsløsninger vil dataene naturlig nok underlegges samme krypteringsregime i hele kjeden, og kryptering vil falle inn under lagringsfasen (fase 2) der anslåtte kostnader skal dekkes av myndighetene.

Som en konsekvens av dette anbefaler PT at drifts- og investeringskostnadene til kryptering før oversendelse hos tilbyder som inngår i en felles lagringsløsning, inngår i de kostnader som skal dekkes av myndighetene.

Refusjon av kostnader ved felles lagringsløsning

Dersom det opprettes en felles løsning for lagring som et betydelig antall aktører slutter seg til, anbefaler PT at det vurderes hvorvidt kostnadene for lagringen kan dekkes av staten direkte ovenfor operatør(ene) av slike løsninger.

Kostnadene til investering og drift av en felles løsning vil uansett måtte fordeles på de tilbydere som er tilsluttet den felles lagringsdatabasen. Det antas at kostnadsandelen for hver lagringspliktige vil bli fastsatt gjennom forhandlinger mellom tilbyderne som er tilsluttet databasen og operatøren av løsningen.

Det vil etter PTs syn kunne oppnås vesentlige administrative forenklinger og besparelser dersom operatører av felles lagringsløsning(er) får dekket sine kostnader direkte fra myndighetene basert på de satser som fastsettes, heller enn at dette må søkes dekket av den enkelte tilbyder tilknyttet basen i etterkant.

Arbeidsgruppe for beregning av refusjonssatser

Det foreslås i høringsnotatets avsnitt 2.5.4 at PT skal lede en arbeidsgruppe for å beregne satser for kostnadsdekning, og at disse skal reguleres gjennom forskrift.

I lys av de mulige konkurransevridende effekter av kostnadsfordelingsmodellen som diskutert overfor, anbefaler PT at arbeidsgruppens mandat gir muligheter for å utarbeide satser for utmåling av kostnadsdekning som kompenserer for slike effekter.

PT ser for seg at en slik arbeidsgruppe bør kunne ha deltagelse fra statlige etater, pliktsubjektene og andre relevante aktører.

Til kapittel 3 «Om politiets uthenting av data i nødsituasjoner»

Generelle merknader

I høringsnotatet foreslås det en ny bestemmelse i ekomloven § 2-9a som skal «synliggjøre politiets rett til å hente ut opplysninger fra tilbyderne» i nødsituasjoner.

PT finner grunn til å kommentere utsagnet i høringsnotatet 3.3.1 om forholdsmessighet, der departementet uttaler at «I situasjoner hvor det er fare for personers liv eller helse vil aldri uthenting av opplysninger fra ekomtilbydere være uforholdsmessig».

Bestemmelsen er åpent formulert og spesifiserer ikke hvilke data som kan besluttet utlevert utover at opplysningene skal være «relevante». I høringsnotatet, og på høringsmøte 22.5.2013, er det uttalt at opplysningene kan være trafikk-, lokasjons- og signaleringsdata fra enkelttelefonnummer, samt tilsvarende data fra basestasjonssøk. PT bemerker at sistnevnte åpenbarer personvernssensitiv informasjon fra en ubestemt og potensielt stor gruppe av tredjepersoner, og at særlige personvern hensyn gjør seg gjeldende.

PT erkjenner at en bestemmelse som skal regulere nødsituasjoner må ta høyde for at mange av de situasjoner som skal reguleres ikke kan vurderes på forhånd. Blant annet på grunn av at avgjørelsene i slike situasjoner regelmessig vil skje under tidspress, er det imidlertid avgjørende å ha foretatt de prinsipielle avveininger som kan gjøres på forhånd. Det savnes i det hele en diskusjon av risikoaksept i høringsnotatet, som kan gi holdepunkter for å foreta den ofte vanskelige avveining mellom personvernet og hensynet til å lokalisere savnede personer.

Gjeldende regelverk og praksis

Straffeloven § 47, som dagens praksis for uthenting av data i nødsituasjoner er forankret i, har tre vilkår for at en ellers straffbar handling likevel er rettmessig. En handling må ha blitt foretatt for å redde noens «person eller gods», i praksis og teori har dette blitt tolket til å gjelde nær sagt enhver interesse. Videre må disse ha blitt reddet fra en «paa anden Maade uafvendelig Fare». I dette ligger det et krav til at andre, lovlige, handlinger har blitt forsøkt eller er åpenbart utilstrekkelige.

Det skal også foretas en forholdsmessighetsvurdering i snever forstand. Omstendighetene må ha berettiget den handlende til å anse faren for «særdeles betydelig» i forhold til den skade som kan forvoldes av nødrettshandlingen. I straffeloven 2005 § 17 er dette uttrykt som at skaderisikoen som avverges «er langt større enn skaderisikoen ved handlingen».

Forslaget til ny bestemmelse synes å være i samsvar med strl. §47 og strl. 2005 §17 for den vernede interessens del, fare for liv og helse. Forholdsmessigheten ved et krav om utlevering av

taushetsbelagte data skal etter forslaget vurderes etter politiloven §6, som ikke setter krav til kvalifisert interesseovervekt.

Videre er det uklart om det etter dagens regelverk oppstår en plikt for tilbyder til å utlevere informasjon underlagt taushetsplikt til politiet der det er påberopt nødrett. Dette er så langt PT kjenner til ikke satt på spissen, da tilbyderne etterkommer alle forespørsler som er tilstrekkelig dokumentert. Etter forslaget skal politiet pålegge utlevering, og det oppstår da en plikt for tilbyderne å etterkomme pålegget.

For PT fremstår bestemmelsen av overnevnte grunner som en betydelig utvidelse av den adgang politiet i dag har til uthenting av trafikk- og lokasjonsdata gjennom nødrettsbestemmelsen i straffeloven § 47.

Bestemmelse om utlevering av taushetsbelagt informasjon i nødstilfeller

Bestemmelsen bør ta høyde for de personvern hensyn som er nevnt ovenfor, blant annet ved å begrense adgangen til utlevering til det omfang som er strengt nødvendig for å finne den eller de det søkes etter. Her kan vises til de nye bestemmelser for utlevering av data i etterforskningen, straffeprosessloven § 210b og § 210c, som begrenser utlevering av data til tilfeller der dette er «av vesentlig betydning for etterforskningen». Det anbefales at en slik begrensning, med nødvendige tilpasninger, inntas i en eventuell ny bestemmelse som regulerer utlevering i nødstilfellene.

Forslaget til ny ekomlov § 2-9a og høringsnotatet for øvrig presiserer ikke om tilfellene nevnt i andre punktum (søk etter savnet person og annet redningsarbeid) er ment å være uttømmende. Det står i det hele åpent om søk etter savnet person og redningsarbeid er ment å være eksempler på når første ledd kommer til anvendelse, eller om den kun er anvendelig i slike tilfeller. Etter PTs syn bør dette klargjøres i selve lovteksten, spesielt siden man her er innenfor legalitetsprinsippets område.

Kontroll med bruk av bestemmelsen

Det bes i høringsnotatet særskilt om kommentarer på hvilke kontrolltiltak som skal gjelde ved utlevering av data etter bestemmelsen. PT viser her til de kommentarer som er gjort i forarbeidene til gjennomføring av datalagringsdirektivet i norsk rett.¹ Her omtales domstolskontroll som en «sentral rettssikkerhetsgaranti».

Forutgående domstolskontroll av politiets bruk av tvangsmidler i forvaltningssporet, utenfor etterforskning og straffeprosessen, er ikke nytt i lovverket. Slike regler er blant annet gitt i politiloven § 17d.

Etter straffeprosessloven § 210b skal det opprettes en vaktordning i Oslo tingrett for å behandle saker om utlevering av trafikk- og lokasjonsdata som ledd i etterforskning. PT anbefaler at utlevering av slike data, også i nødsituasjoner, som hovedregel skal underkastes forutgående domstolsbehandling. Politiet kan gis hastekompetanse der det ikke er tid til å innhente domstolens avgjørelse.

¹ Innst. 275 L (2010-2011).

Til kapittel 4 «PUK-koder og kundereskontro»

PT stiller seg bak de vurderinger som er gjort om å presisere i lov at PUK-koder er omfattet av taushetsplikten.

Høringsnotatet inneholder noen bemerkninger om utlevering og lagring av signaleringsdata. I lys av de personvern hensyn som gjør seg gjeldende, fører PT i dag en restriktiv praksis for fritak fra tilbyders taushetsplikt for denne type data. I særdeleshet praktiserer PT en høy terskel for å gi fritak fra taushetsplikten for signaleringsdata fra basestasjonssøk. PT vil, inntil Samferdselsdepartementet kommer tilbake med forslag til lovendring, fortsette med dagens praksis.

Med hilsen

Torstein Olsen
direktør

Einar Lunde
avdelingsdirektør