Kommunal- og moderniseringsdepartementet
Postboks 8010 Dep
0030 Oslo

Sendes kun elektronisk til
postmottak@kmd.dep.no

Vår dato
22.01.2021

Vår referanse
2021-239

Deres dato
09.10.2020

Deres referanse
20/3645-1

Vår saksbehandler
Pål V. Pettersen m. fl.

Vedr. endringer i ekomloven (lagring av IP-adresser mv.)

Telenor Norge AS (heretter Telenor) viser til mottatt høringsnotat vedr. forslag om å innføre en plikt for tilbydere av ekomtjenester til å lagre IP-adresser, datert 9. oktober 2020, og takker for muligheten til å komme med våre innspill til denne saken. Vi har tidligere bidratt til de respektive departementene med informasjon i forarbeidet til høringsnotatet, og stiller oss gjerne til disposisjon for ytterligere tekniske avklaringer mv.

Overordnede kommentarer
Den økende bruken og samfunnets avhengighet av elektronisk kommunikasjon, tilsier en tilsvarende vektlegging av kommunikasjons- og personvern. Telenor er enig med departementene i at «[e]n plikt til å lagre IP-adresser som gir abonnementsopplysninger/brukerdata, er langt mindre inngripende for kommunikasjonsvernet enn en lagringsplikt for alle trafikkdata, som gir langt mer informasjon». Like fullt representerer departementenes forslag en inngripen i person- og kommunikasjonsvernet. Vi noterer oss at departementene innledningsvis eksplisitt anerkjenner at «det er utfordrende å finne en riktig balanse mellom kriminalitetsbekjempelse og behovet for kommunikasjonsvern og personvern». Det er etter vår oppfatning viktig at denne erkjennelsen preger arbeidet med det evt. endelige forslaget.

Vi registrerer en utvikling der ekomtilbyderes data i større og større grad etterspørres av myndighetene for ulike formål. Summen av ekom-informasjon som lagres – og som kan spores til den enkelte borger – er etter hvert betydelig, og etter alt å dømme voksende i takt med den teknologiske utviklingen. Det er avgjørende at departementene i det videre arbeidet med saken ser dette i sammenheng, også hensyntatt det pågående arbeidet til den regjeringsoppnevnte Personvernkommisjonen som skal levere sin utredning innen utgangen av 2021.

For Telenor er person- og kommunikasjonsvernet både en grunnleggende samfunnsverdi og et viktig premiss for vår virksomhet. Våre kunder skal ha tillit til at de trygt kan kommunisere gjennom våre nett. Telenor ønsker ikke å lagre mer informasjon om våre kunders data- og telefonbruk enn hva vi trenger for å kunne oppfylle vår kontrakt med den enkelte kunde, og for å kunne tilby kunden best mulig tjenester både i dag og i fremtiden. Det vil være skadelig for

vår virksomhet dersom våre tjenester oppfattes å utfordre person- og kommunikasjonsvernet, og ei heller ønskelig i et samfunnsperspektiv.

Samtidig erkjenner vi politiets behov for oppdaterte verktøy i en digital hverdag, slik vi også indikerte i forbindelse med vårt høringssvar vedr. innlemmelsen av Datalagringsdirektivet i norsk rett for 10 år siden. I høringssvaret understreket vi vårt prinsipale standpunkt om at direktivet *ikke* burde innlemmes i norsk rett, og vi påpekte at alternativene til full implementering ikke var tilstrekkelig belyst:

«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.»

Telenor ønsker å bidra til å finne løsninger som balanserer ovenstående hensyn. Vi vil imidlertid understreke at dersom forslaget om IP-lagring fremmes bør det rammes tydelig inn bl.a. mht. person- og kommunikasjonsvern, utlevering av opplysninger, samt en kostnadsfordelingsmodell som ikke legger en urimelig byrde på den enkelte Internet Service Provider (ISP). Regelverket må være treffsikkert og tydelig, det må bidra til at man unngår at det lagres og utleveres flere opplysninger enn hva som er nødvendig for å oppfylle formålet, og data må være sikre.

I det følgende gir vi – med utgangspunkt i vår virksomhet – et utvalg kommentarer til sentrale deler av høringsnotatet.

Diverse tekniske vurderinger og problemstillinger

Telenor merker seg at departementene – med rette – understreker at det gjennom ulike krypterings- og anonymiseringsløsninger er mulig å skjule sin identitet på nettet. En lagringsplikt, slik som foreslått, vil dermed kunne omgås, og vil således kunne ha begrenset verdi for formålet. Vi tar til etterretning at departementene legger til grunn at en lagringsplikt «samlet sett likevel vil ha stor verdi for kriminalitetsbekjempelsen».

Departementene anfører i notatet at «[l]agring av IP-adresser omfatter ikke lagring av informasjon om innholdet i abonnentens internettkommunikasjon, hvem abonnenten har vært i kontakt med, eller hvor abonnenten befinner seg.» Vi vil i denne forbindelse gjøre oppmerksom på at dersom IP-adressen er tilknyttet et fastnett-abonnement (dvs. en fysisk linje – for eksempel kobber eller fiber), vil informasjonen vedrørende IP-adresse og bruker i tillegg også (i de fleste tilfeller) kunne gi informasjon direkte/indirekte om fysisk lokasjon/plassering for terminerende ende av den fysiske linjen (dvs. installasjonsadresse for kundens abonnement) via kundedata. Det vil med andre ord avsløre hvor abonnenten har befunnet seg når vedkommende benyttet den etterspurte IP-adresse.

I tilfellene hvor abonnenter deler IP-adresser (NAT-løsning) omtales det i notatet et behov for at politiet skal få tilgang til et «tilstrekkelig presist angitt kommunikasjonstidspunkt». På generelt grunnlag – og uavhengig om det er NAT-løsning eller ikke – vil vi gjøre oppmerksom på at det kan være en utfordring at «timestamp» som politiet anmoder om kan være forskjellig fra «timestamp» hos den enkelte ISP. Dette er en potensiell feilkilde som er viktig å være klar over.

Når det gjelder NAT-løsninger generelt ber departementene høringsinstansene besvare «…om det er mulig å unngå å bruke NAT-løsninger som innebærer at man også må lagre destinasjonsinformasjon. Alternativt dersom dette ikke kan unngås, for eksempel når standardiserte løsninger benyttes, om det i så fall kan tilpasses løsninger som hindrer lagring av eventuell destinasjonsinformasjon.» Det finnes så vidt vi kjenner til ingen NAT-varianter der man også må lagre destinasjonsinformasjon.

Departementene skriver videre at de ikke er «kjent med at det i dag brukes løsninger hvor det er behov for å lagre ytterligere informasjon for å kunne identifisere en abonnent (for eksempel portnummer på destinasjonssiden), men ber om høringsinstansenes innspill på om slike løsninger er i bruk.» Telenor har ingen nettverksmodeller (som f.eks. statisk IP, NAT, CGNAT, NAT64) i bruk som krever lagring av data om destinasjonssiden for dette formål.

Telenor vil på generelt grunnlag understreke at hvis en ISP må lagre offentlig IP-adresse/offentlig port/start-tidspunkt/slutt-tidspunkt, så vil en forespørsel fra politiet på offentlig IP-adresse/offentlig port/tidspunkt alltid gi et unikt svar. En forespørsel på offentlig IP-adresse/offentlig port vil alltid gi settet av abonnenter som deler den offentlige IP-adressen på tidspunktet. Hvor mange abonnenter som deler på offentlige IP-adresser til enhver tid, kommer an på hvor mange offentlige adresser ISP-en eier og bruker på CGNAT-løsningen. Dette er konfigurerbart hos den enkelte ISP.

Telenor vil for øvrig gjøre oppmerksom på at det kan være utfordringer med å finne riktig bruker av en IP-adresse, dersom det er flere ledd med NAT-ing i kommunikasjonskjeden. Et eksempel på sistnevnte kan være tilfeller hvor wholesalekunde/tjenestetilbyder med egen NAT-løsning leier kapasitet hos en nettoperatør som også benytter en egen NAT-løsning.

Vi vil understreke at det verken er mulig eller ønskelig for Telenor å hente ut abonnementsopplysninger for tjenestetilbydere som benytter Telenor sine nett. I så tilfelle må politiet henvende seg til den aktuelle tjenestetilbyder for å få utlevert nevnte opplysninger. Politiet finner den aktuelle tjenestetilbyder ved å bruke RIPE.

Regler om lagringsplikt

Hvem skal lagre?
Departementet legger til grunn at alle tilbydere som tilbyr tjenester hvor sluttbruker gis tilgang til internett skal pålegges en lagringsplikt – dvs. at ISPer skal lagre informasjon slik at det er mulig å koble en IP-adresse til en spesifikk internettaksess-abonnent. Dette er etter Telenors oppfatning en fornuftig måte å definere pliktsubjektene på, siden det er den enkelte ISP som har en relasjon til sine abonnenter. Dette prinsippet må også gjelde i de tilfellene ISPen ikke selv drifter en løsning for IP-allokering, eller innenfor ulike modeller i grossistmarkedet.

En fornuftig praksis i slike tilfeller vil etter Telenors oppfatning være at politiet i første instans innhenter informasjon fra internettoperatøren som «eier» relevant IP-adresse, og deretter får opplyst hvilken tjenestetilbyder som innehar abonnenten – jf. omtale av RIPE over. Politiet gjør så en anmodning til riktig tjenestetilbyder for å få utlevert abonnementsopplysninger. Vi mener videre arbeid med saken må tydeliggjøre hvordan dette skal foregå, jfr. også omtale under vedr. utlevering av opplysninger.

Hva skal lagres?

I høringsnotatet fremkommer det at selve lagringsplikten kan presiseres slik at det «… skal lagres de opplysninger som er nødvendige for å identifisere abonnenten ut ifra:

a) en IP-adresse og et tidspunkt for kommunikasjon, eller

b) en offentlig IP-adresse, et tidspunkt for kommunikasjon og portnummer benyttet ved kommunikasjonen, dersom samme offentlige IP-adresse tildeles flere abonnenter samtidig.»

Telenor mener det er viktig at ISPene selv gis rom for å definere hva som er nødvendige dataelementer å lagre for å identifisere en abonnent ut fra ovenstående, og at dette ikke behøves regulert ytterligere fra myndighetenes side. Avhengig av systemkonfigurasjon og nettverksmodell vil det også være ulikt behov for informasjon om en abonnents trafikk for å kunne identifisere vedkommende.

Hvem, hvordan og hvor skal data lagres?
Telenor er enig i at videreføring av dagens krav til sikkerhet er et godt alternativ ved innføring av lagringsplikt. Telenor er i dag underlagt krav som følger av ekomloven, sikkerhetsloven og GDPR. Det er den enkelte ISP som vil måtte være ansvarlig for denne sikkerheten uavhengig om dette gjøres internt i bedriften, eller ved hjelp av underleverandører. Det bør ikke komme noen myndighetspålegg ut over dette, inkludert eventuelle pålegg om felles lagringsløsning.

Lagringstid
Slik indikert innledningsvis mener Telenor at det er tungtveiende grunner for at departementene legger til grunn det minst inngripende alternativet mht. person- og kommunikasjonsvern dersom forslaget fremmes. Ut fra høringsnotatets drøftinger vil dette innebære seks mnd. lagringstid.

Utlevering og bruk av opplysninger
Telenor mener – hensyntatt forslagets uttalte formål om å bekjempe «alvorlig kriminalitet» – at mye taler for at adgangen til utlevering av opplysninger bør begrenses enten ved en minimumsterskel for strafferamme og/eller å begrense utleveringen til forebygging og etterforskning av bestemte straffebud. Samtidig vil vi understreke at vi ikke tar stilling til hva som bør være det materielle innholdet i disse kravene. Påtalemyndighetene må påvise en klar hjemmel, og en slik utvidet lagring for kriminalitetsbekjempelse må ikke få betydning i sivile saker.

Telenor merker seg at departementene vurderer det dithen at vilkårene for utlevering av opplysningene som skal lagres etter forslaget, strammes inn sammenlignet med gjeldende rett for å ivareta kravet om proporsjonalitet etter Grunnloven, EMK, kommunikasjonsverndirektivet og EØS-retten. Telenor støtter dette synet, og er enig i at en innstramming er nødvendig. Det bør tilstrebes å få klarest mulig regler om dette – inkludert tydelige retningslinjer for nødvendighetsvurderinger – slik at en innstramming ikke blir illusorisk i praksis, eller at ISPene må bruke betydelige ressurser for å ivareta sin taushetsplikt og kommunikasjonsvernet for sine abonnenter.

Vi mener også at ekomtilbydere bør motta en anmodnings-verifikasjon fra påtalemyndighetene og at man får informasjon om hvilken hjemmel – f.eks. hvilken bestemmelse i straffeloven og straffeprosessloven – som ligger til grunn for en utleveringsanmodning. Generelt vil vi minne om at lovmessige utvidelser som gir myndighetene økte muligheter for innsyn, bør følges opp med transparens omkring faktisk bruk av disse.

Departementene etterspør særskilt høringsinstansenes syn mht. bruk av opplysninger om IP-adresser i sivile saker, og om det kan være behov for begrensninger på bruken av opplysninger som omfattes av utvidet lagring i sivile saker. Telenor ser faren for formålsutglidning, og vil henvise til det som innledningsvis anføres som departementenes uttalte formål med forslaget – nemlig «å bekjempe alvorlig kriminalitet». Forslaget bør rammes inn ift. dette.

Generelt vil vi, i likhet med høringsnotat, minne om at det alltid er en viss risiko for at data som ekomtilbydere utleverer politiet kan være beheftet med feil eller mangler, både fordi data ikke er samlet inn for dette formålet og fordi ulike typer av feil kan oppstå. Særlig ved arbeid i nettet og ved feilsituasjoner så kan oppdateringer bli forsinket og/eller gå tapt, og med det redusere datakvaliteten.

Kostnadsfordelingsmodeller
Prinsipielt mener Telenor at det i tilfeller hvor staten pålegger private aktører utvidede oppgaver av ulik art, så bør også staten ta kostnadene både for investering og drift i tilknytning til disse.

I forlengelsen av dette er det etter vår oppfatning behov for en mer prinsipiell avklaring av hvordan kostnadsfordelingen skal være i forbindelse med myndighetspålegg i den digitale infrastrukturen. Blant annet burde dette gjelde alt som er omfattet av ekomloven §2-8 («Tilrettelegging for lovbestemt tilgang til informasjon») fra spesifikke lagringssystemer til kommunikasjonskontroll.

Når det gjelder f.eks. etablering av løsning/system for kommunikasjonskontroll jf. ekomloven § 2-8 har ikke tilbyderne noe behov/formål for et slikt system – det er det staten som har. Likevel har aktører som Telenor måttet dekke alle investeringskostnader relatert til dagens ordning, mens driftskostnadene i stor grad har blitt dekket av politiet. Telenor har ved flere tilfeller etterlyst klarere føringer mht. kostnadsfordeling i tilknytning til kommunikasjonskontroll, uten at vi så langt har lyktes med å få en omforent forståelse mellom Telenor og politiet vedr. hvem som skal dekke hva.

Ovenstående bør departementene – også uavhengig av dette høringsnotatet – søke en klargjøring av.

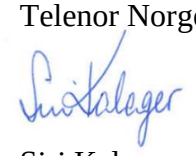
Vi merker oss de ulike alternative kostnadsfordelingsmodellene som fremkommer av høringsnotatet. Ingen av de foreslåtte modellene er – etter vår oppfatning, hensyntatt ovenstående prinsipielle utgangspunkt – tilstrekkelig dekkende. I et valg mellom dem ser imidlertid Telenor det som aktuelt å kunne diskutere videre med departementene ut fra alternativ D skissert i notatet, under forutsetning av at private aktører ikke pålegges en urimelig byrde: «Investeringskostnader deles mellom staten og tilbyderne i henhold til en fordelingsnøkkel. Staten dekker faste driftskostnader og uthentingskostnader». En evt. tydeliggjøring av fordelingsnøkkelen mellom stat og tilbydere bør ta utgangspunkt i tilbyders eksisterende investeringer. Vi understreker at vi er særlig opptatt av at merkostnadene knyttet til drift – og en omforent avklaring av hva som skal defineres som «merkostnader» – dekkes av staten. Dette gjelder både faste driftskostnader og uthentingskostnader.

Mht. høringsnotatets diskusjon vedr. automatisering og forenkling på tilbyders hånd – for eksempel med en API-lignende ordning i forbindelse med selve utlevering til politiet – vil Telenor understreke at dette ikke bør pålegges ISPene. Når det gjelder fokus på det interne arbeidet med å tilrettelegge for en effektiv og rask fremhenting av informasjonen fra systemene,

stiller Telenor seg positiv til automatisering og forenkling i den grad dette er praktisk gjennomførbart.

Vi stiller oss gjerne til rådighet ved behov for ytterligere informasjon.

Med hilsen
Telenor Norge AS



Siri Kalager
Leder myndighetskontakt og regulatorisk