Høringsuttalelse – Endringer i ekomloven (lagring av IP-adresser)

Den internasjonale juristkommisjon – norsk avdeling (ICJ-Norge) viser til Kommunal- og moderniseringsdepartementet og Justis- og beredskapsdepartementets høring 9. oktober 2020 med forslag om å innføre en plikt for tilbydere av ekomtjenester til å lagre IP-adresser. Formålet er at politiet kan få tilgang til IP-adressene for å bekjempe alvorlig kriminalitet.

1. Innledning

ICJ vil innledningsvis bemerke at helhetsinntrykket av høringsnotatet er positivt. Notatet fremstår som grundig og gir en nokså dekkende utredning av en slik lovendring og konsekvensene det vil medføre. Det er samtidig noen svakheter ved høringsnotatet, som ICJ vil kommentere i det følgende.

2. Kommentarer til høringsnotatet

2.1 Utredning av personvernkonsekvenser

Det er ICJ sin vurdering at en lovbestemmelse som i dette tilfellet, forutsetter en utredning av personvernkonsekvenser iht. personvernforordningen art. 6, 3. ledd og utredningsinstruksen.. Utredningsinstruksen krever at hver sak skal inneholde en konsekvensutredning som skal bestå av analyse og vurdering av antatte vesentlige konsekvenser av den beslutning som foreslås truffet.

En nasjonal hjemmel for behandling av personopplysninger som her foreslås, må oppfylle et mål i allmennhetens interesse og stå i et rimelig forhold til det berettigede målet som søkes oppnådd. Personvernkonsekvensvurderingen må derfor utrede særlig følgen av lagringslengde, volum, koblingsmuligheter til andre datakilder m.m.

Lagringsplikt vil da bare være tillatt såfremt inngrepet ivaretar et legitimt formål, har tilstrekkelig hjemmel og er forholdsmessig.

Nedkjølingseffekt

ICJ savner blant annet en grundigere drøftelse av nedkjølingseffekten en slik lagrinsplikt kan medføre. Departementet er inne på problemstillingen i punkt 7.1.3, og reiser spørsmålet om lagring av IP-adresser kan ha en nedkjølende effekt på ytringsfriheten. Dette mener vi ikke er vurdert i tilstrekkelig grad. Departementet peker på at individet ikke automatisk kan identifiseres, men det er nettopp det man ønsker ved en slik lagringsplikt; å identifisere personen bak IP-adressen.

Forholdsmessighet

På side 2 i notatet påpeker departementet at «(...)Uthenting av lagrede IP-adresser vil like fullt være et svært viktig verktøy i arbeidet mot kriminalitet. For at tiltaket skal bli effektivt og målrettet også når en tilbyder tildeler samme IP-adresse til flere abonnenter samtidig, foreslås det at tilbyder i slike tilfeller også skal lagre informasjon om hvilke portnumre på abonnentsiden som er benyttet ved kommunikasjonen.»

Videre på side 22 forklarer departementet at det vil være vanskelig å identifisere en person kun ut fra en IP-adresse uten nærmere etterforskning. I tillegg vil en bruker lett kunne skjule sin identitet ved bruk av VPN eller annen kryptering. Departementet konkluderer likevel med at lagring av IP-adresser vil være et effektivt verktøy i politietterforskninger, uten at den antatte effekten av f.eks. VPN drøftes videre.

Dette reiser følgende spørsmål: Er virkemiddelet effektivt for bekjempelse av kriminalitet, til tross for at det er enkelt å skjule seg bak kryptering, for eksempel VPN?

En generell og udifferensiert lagring av alle IP-adresser er et stort inngrep i personvernet. For at det skal være rettferdiggjort må det være forholdsmessig og nødvendig i et demokratisk samfunn. Effektiviteten (eventuelt ineffektiviteten) av en slik lagringsplikt står sentralt i vurderingen. Et ineffektivt virkemiddel vil fort kunne bli ansett som uforholdsmessig inngripende.

Bevisbyrden ligger på lovgiver for å begrunne effektivitet versus lagringstid og treffsikkerhet. Personopplysninger skal være korrekte, og det er verdt å nevne at treffsikkerheten vil kunne forringes med lengre lagringstid. Faren for ukorrekte opplysninger vil øke etter hvert som tiden går. Slik informasjon har et element av «ferskvare»-kvalitet ved seg.

Departementet går ikke nærmere inn på problemstillingene, men konkluderer med at dette vil være et viktig og effektivt verktøy for politietterforskning. ICJ reiser spørsmålet om det er mulig å innhente dokumentasjon som underbygger departementets påstand.

2.2 Mengden data – Riktig fortolkning av EU-domstolens avgjørelser?

Departementet henviser til ulike avgjørelser fra EU-domstolen når de diskuterer lovligheten av en plikt til å lagre IP-adresser. ICJ stiller seg imidlertid spørrende til om departementet har utredet problemstillingen grundig nok.

I Tele2-dommen kom EU-domstolen til at en generell og udifferensiert datalagring av alle trafikk- og lokasjonsdata om alle abonnenter og registrerte brukere er ulovlig (se gjennomgang av dommen på side 13-14 i høringsnotatet). Domstolen åpnet imidlertid for at målrettet datalagring kan være lovlig, forutsatt

at lagringen er begrenset med hensyn til personer, kommunikasjonsmidler, kategorier av data som lagres og lagringstid (ref. side 14 i høringsnotatet og avsnitt 108 i nevnte dom).

I avsnitt 108 i dommen uttaler EU-domstolen at målrettet datalagring kan være i tråd med EU-retten, «forudsat at lagringen af disse data begrænses til det strengt nødvendige for så vidt angår kategoriene af data, der skal lagres, de omhandlede kommunikationsmidler, de berørte personer og den fastsatte varighed af lagringen».

Departementet påpeker på side 14 i notatet at «det er imidlertid noe uklart hvorvidt lagringen må begrenses med hensyn til både opplysningskategorier, kommunikasjonsmåter, berørte personer og lagringstid, eller kun noen av disse».

I litteraturen er det imidlertid argumentert for at EU-domstolen oppstilte 4 *kumulative* vilkår i Tele2-dommen, og følgelig at datalagringen må være begrenset med hensyn til alle fire vilkår. (Ref. uttalelsen til generaladvokat Henrik Saugmandsgaard Øe, som skrev forslag til avgjørelse i Tele 2 – saken, under en workshop i 2017.[1] Se også Sophie Stalla-Bourdillon, "The CJEU in Tele2 Sverige: are general(ised) data retention obligations incompatible with EU law?" (2017)[2]) En slik forståelse underbygges også av ordlyden; «(...)de berørte personer *og* den fastsatte varighed af lagringen.». (egen utheving)

Departementet går ikke nærmere inn på spørsmålet, men mener at lagring av IP-adresser er rettferdiggjort, og referer til La Quadrature de Net-dommen. I avsnitt 155 i dommen uttalte EU-domstolen at en generell og udifferensiert lagring av IP-adresser ikke i prinsippet er i strid med kommunikasjonsverndirektivet og EU-pakten (se s. 15 i notatet).

Det hadde imidlertid vært interessant å vurdere EU-domstolens vurdering av IP-adresser i Le Quadrature de Net-dommen, i sammenheng med domstolens uttalelse om vilkårene for målrettet lagring av trafikk- og lokaliseringsdata i Tele2-dommen. Dette er en uttalelse som for øvrig ble gjentatt av domstolen i le Quadrature de Net hva gjelder lagring av trafikk- og lokaliseringsdata (ref. avsnitt 147 i dommen).

I Le Quadrature de Net åpner EU-domstolen for at generell lagring av IP-adresser kan være lovlig, men hvordan samsvarer dette med EU-domstolens uttalelser om vilkårene for målrettet datalagring av trafikk- og lokasjonsdata? IP-adresser utgjør også en form for trafikkdata. Ved å lagre alle IP-adresser, men ikke noe annet, så vil det medføre begrensning i kategorier av data som lagres, kanskje også kommunikasjonsmidler, i tillegg vil lagringstiden være begrenset. Det gjøres imidlertid ingen begrensning i personene som blir berørt av datalagringen, ettersom en generell og udifferensiert lagring vil ramme alle brukere/abonnenter. Hvordan dette harmonerer med EU-domstolens uttalelser om å begrense antall berørte personer er en interessant problemstilling å se nærmere på, hvilket vi ikke kan se at departementet har gjort.

[1] E-volution of Data Protection Conference Workshop 2 – Privacy vs. Security. Foredraget til Saugmandsgaard Øe ble filmet, se fra 52:57 (min:sek) av videoen

[2] https://peepbeep.wordpress.com/2017/01/04/the-cjeu-in-tele2-sverige-are-generalised-data-retention-obligations-incompatible-with-eu-law/

2.3 Bevissikring i sivile saker/Tilgang til data

En problemstilling er eventuell tilgang til lagrede data i sivile saker. Departementet har ikke foreslått noen innstramminger, men ber om innspill (se nederst på side 39). Riktignok krever den sivile tilgangen samtykke fra Nkom eller rettslig kjennelse, men i prinsippet kan da parter i sivile saker få tilgang til taushetsbelagt informasjon, som for politiets vedkommende begrenses til bekjempelse av alvorlig kriminalitet. Dette er særlig aktuelt ved bevissikring utenfor rettsak.

Rettsdatas kommentar til tvistelovens § 28-4, om gjennomføring av bevissikring utenfor rettssak («reglene i rettssak gjelder så langt de passer»), sier følgende:

> *Det gis ingen nærmere anvisning på hvordan bevissikring praktisk skal gjennomføres. Lovgiver har ikke tatt stilling til praktiske og prinsipielle problemer ved bevissikring utenfor rettssak, særlig når dette skal gjennomføres uten varsel til motparten, hvor rettens beslutning ligger nær beslutning om ransaking i straffeprosessen. Det er uklart hvilke virkemidler som står til disposisjon for å få tilgang til bevisene som skal sikres. Retten kan gi pålegg om utlevering, og den som skal gjennomføre sikringen kan komme uanmeldt, men det foreligger ingen hjemmel for å benytte tvang til gjennomføringen. Det følger forutsetningsvis av Rt. 2006 s. 626 at bevissikringsretten kan få bistand fra namsfogden til gjennomføringen. Når motparten ikke varsles, kan tingretten eksempelvis be namsmannen (og med de medhjelpere som namsmannen finner hensiktsmessig) gjennomføre bevissikringen og registrere og deponere det bevissikrede materialet. […]*

Høyesterett har i Rt. 2010 s. 774 avsnitt 42 uttalt at det «passer» å benytte tvl. § 22-3 annet og tredje ledd, om at bevis likevel kan føres på tross av lovbestemt taushetsplikt, også i sak om bevissikring. Det kan imidlertid tenkes tilfeller hvor prosessen for bevissikring innebærer at også reglene om bevisforbud og bevisfritak må praktiseres noe annerledes enn normalt. Illustrerende er LB-2011-54359 (jf. HR-2012-684-U): Lagmannsretten hadde sluttet seg til at et sikret datamateriale først skulle gjennomgås av en rettsoppnevnt sakkyndig. Når den sakkyndiges rapport forelå skulle denne fremlegges for tingretten, som måtte avgjøre konkret i hvilken grad reglene om bevisfritak var til hinder for at bevisene ble gjort kjent for saksøker

Det er på bakgrunn av denne noe uklare rettstilstanden at mengden av tilgjengelig informasjon eventuelt skal utvides i sivile saker. Politiet på sin side er underlagt blant annet politiregisterloven i sin senere behandling av opplysningene.

ICJ er skeptisk til det sivilrettslige bildet i forbindelse med lagring av IP-adresser, og frykter at en generell lagring over mye lengre tid enn det i dag er praktisert, vil kunne gjøre det mulig for sivile å få tilgang på IP-adresser i mye større grad enn tidligere. En slik aksessorisk åpning/lagring vil potensielt ramme småbrukere, noe som er meget uheldig, og som går langt utover formålet med lovendringen. Se for

eksempel høyesterettsdom HR-2017-833-A, hvor rettighetshaverne til filmen «Max Manus» ønsket å få utlevert IP-adresser til filbrukere som hadde ulovlig lastet ned filmen. Begjæringen ble avslått. Dersom lagringstiden blir vesentlig større, er det mye større behov for å regulere hvem og hvordan denne informasjonen kan tilgjengeliggjøres, for å forhindre at informasjon om IP-adresser blir «allemannseie».

Det er derfor særlig viktig at det er strenge reguleringer omkring hvem som har tilgang til lagrede IP-adresser, også utenfor politi og påtalemyndighet. I tillegg må lagringen formålsbegrenses, også for de aktører som pålegges lagringen opprinnelig. Slik ICJ-Norge forstår nevnte avgjørelse i Le Quadrature de Net, er det *kun* kriminalitetsbekjempelse som formål som eventuelt kan rettferdiggjøre en lagringsplikt. Tilgang i sivile saker, særlig på et så upresist rettsgrunnlag som i dag, kan dermed medføre at hele lagringsregimet underkjennes på EU/EØS-rettslig grunnlag.

2.4 Alvorlighetsgrad og strafferamme

Når det gjelder alvorlighetsgraden av kriminelle forhold som skal gi politiet tilgang, foreslår departement prisverdig nok en tilstramming i forhold til dagens regelverk (nederst på side 33), hvor det for politi og påtalemyndighet ikke er gitt terskler i gjeldende rett.

Vedrørende strafferammen til disse forholdene ønsker ICJ å stille følgende spørsmål: Hvorfor skal den samme EU-rettslige terskel om alvorlig kriminalitet vurderes annerledes nå enn ved Stortingets vedtak om innføring av datalagringsdirektivet? Dersom departementet anser at det gjelder en annen terskel for hva som utgjør alvorlig kriminalitet etter EU-retten nå enn ved vedtaket om innføring av datalagringsdirektivet, bør dette kommenteres nærmere.

Personopplysninger som f.eks. IP-adresser skal ikke lagres uten et spesifikt formål. Det er derfor viktig at det er klart definert hva som menes med «alvorlig kriminalitet».

Med vennlig hilsen

Sign. Erlend Balsvik
Faggruppeleder

Sign. Terje Einarsen
Styreleder


icj
International
Commission
of Jurists