Postboks 27 Vålerenga
0626 Oslo

Kommunal- og moderniseringsdepartementet og
Justis- og beredskapsdepartementet
Postboks 8010 Dep
0030 Oslo

HØRINGSUTTALELSE - ENDRINGER I EKOMLOVEN (20/3645-1)

Elektronisk Forpost Norge har mottatt høringsnotatet [1] om endringer i ekomloven fra kommunal og moderniseringsdepartementet og justis og beredskapsdepartementet. Vi vil her komme med synspunkter og kommentarer til forslaget.

Elektronisk kopi av dette dokumentet er sendt inn elektronisk via linken som ble oppgitt i høringsnotatet [2]

OVERSIKT OVER EFNs HØRINGSUTTALELSE

Vi har lest Departementets høringsdokumenter og inndelt vår høringsbesvarelse logisk innen de temaer vi gir besvarelse for, og som vi mener er viktig å gi tilbakemelding om.

Den viktigste tilbakemeldingen vi har er:

Med departementets forslag om bevissikring i form av IP-adresser representerer en akkumulering og lagring av befolkningens nettbruk som i realiteten representerer kartlegging av en stor del av nett- og mobil-brukers nettaktiviteter siste 6 til 12 måneder. Samlingen av trafikkdata som foreslås vil i realiteten gi oversikt over hvem snakker med hvem eller hvem gjør hva, hvor og når. Det må derfor anses som et svært strengt inngrep i privatlivet og vi kan ikke se at fordelene ved slik bevissikring er større enn ulempene de gir.

Rent teknisk og juridisk finner vi lovforslaget diffust med hensyn til at konkrete bestemmelser om hva som skal lagres gis ved forskrift, senere.

Tilsvarende for formålet med lagringen, som ikke er avgrenset men omfatter alt fra kriminalitetsforebygging til sivile rettssaker, den foreslåtte strafferammen som skal brukes for å avgrense denne typen bevissikring er også foreslått svært lav, ett til to år. Det vil omfatte svært mye kriminalitet. I praksis vil nok kun fyllekjøring med moderat promille være unntatt.

Der spesifiseres ingen krav til lagring eller hvordan dataene om brukerne kan benyttes, da dette baseres seg på selvbetjening fra politiet, uten domstolskontroll eller andre krav utover at politiet selv er ansvarlig for hva de mener de trenger.

Generelt finner vi departementets argumentasjon tilhørende en tid rundt 25 år tilbake. Vi har derfor tillatt oss å peke til dagens problematiske situasjon og veien videre litt fremover, for løsninger som er mer i tråd med klimaforpliktelser, mer personvernvennlige, og som er ønskelige også for politiets ønsker om etterforskningsmetoder og muligheter.

Innholdsfortegnelse

Om EFN

EFN er en digital rettighetsorganisasjon. Vi jobber for at menneskerettigheter skal ivaretas i det digitale samfunn. EFN består av ulønnede medlemmer med hovedsakelig IT, jus og biblioteks-bakgrunn, men vi har også andre medlemmer fra et vidt spekter av yrkesgrupper. Politisk spenner vi over alle partier representert på stortinget. Internasjonalt er EFN en del av European Digital Rights (EDRi) og deltar aktivt i prosesser innenfor bl.a. EU, Europarådet og FN.

I den foreliggende saken er det satt ned et høringsutvalg bestående av Britt Lysaa og Bjørn Remseth.

Vi har inndelt vårt høringstilsvar i punkter, relatert Departementets Høringsbrev, og kommenterer under hvert av disse punktene:

Noen prinsipielle betraktninger

Det er tre viktige prinsipielle problemstillinger vi mener denne lovendringen berører:

- *Nedkjølingseffekt*: Det at en økt overvåkning fører til at informasjonsutveksling i samfunnet, både offentlig og privat, blir mindre åpen fordi man rettmessig kan tro at det man sier og gjør i økende grad blir overvåket av statlige organer som aktivt leter etter ting man sier og gjør som kan gjøre at man selv eller noen man kjenner kommer under mistanke for straffbare handlinger. Et spesielt og alvorlig spesialtilfelle av nedkjøling er svekkelse av konfidensialitet. Dette omfatter blant annet kildevern for journalister, beskyttelse av konfidensialitet for kommunikasjon mellom advokater og deres klienter, fri utøvelse av fagforeningsvirksomhet, kommunikasjon internt i religiøse grupper og varslere rent generelt. Man kan kanskje argumentere for at det finnes tekniske løsninger som gir godt vern for disse gruppene, men det gjelder ikke alle. Det vil dermed være slik at enhver akkumulering av brukerdata og/eller overvåkning går spesielt utover de svakeste gruppene, altså de som trenger mest beskyttelse.
- *Uskyldspresumsjonen*: I et liberalt rettssamfunn er det en grunnleggende forutsetning at enhver antas å være uskyldig inntil det motsatte er bevist. I Norge er dette grunnlovsfestet i Grunnlovens paragraf §96. Uskyldspresumsjonen ligger også tungt bak Grunnlovens paragraf §102 «*Enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin kommunikasjon. Husransakelse må ikke finne sted, unntatt i kriminelle tilfeller*.» Det er derfor utvilsomt slik at der undersøkelser med formål å avdekke kriminelle handlinger, uten spesiell mistanke om at slike handlinger er begått, i beste fall er i potensiell konflikt med uskyldspresumsjonen.

- *Formålsglidning*: Det er er lett å bli litt oppgitt når man leser slike forslag som dette. Årsaken er følgende resonnement:

    - Det ønskes, med referanse til terrorister, torturister og pedofile, å kunne kartlegge bruk av internett-trafikk for å stoppe de overnevntes aktivitet.

- Konkret settes det imidlertid en beskrankning gitt av strafferammen, og den er ikke høy, ett til to år i følge departementets forslag [1, side 35]. Det settes heller ikke noen beskrankning i forhold til sivile saker, så både straffesaker og sivile saker kan utløse utlevering av data. Brudd på taushetsplikt, (strl § 211), deltagelse i opptøyer (strl §182), hatefulle ytringer (strl §185), unnlate å avverge et straffbart forhold (strl §196), Uberettiget skaffe seg et passord man ikke skulle ha tilgang til (str. §201) o.s.v. Lov om opphavsrett har flere bestemmelser med strafferamme opp til ett år eller mer, så er man mistenkt for den type lovgiving kan og data utleveres. Det er rett og slett en ganske stor andel av Norges lover man nå ønsker å skaffe seg en ny etterforskningsmetode til. Terrorister, torturister og pedofile må antas å være en ganske liten andel av dem departementets forslag vil gi anledning til å forfølge via IP-adresser.
- For å kunne brukes som bevis, er det nødvendig å koble IP-adresse/abonnementsdata mot andre kilder som viser både hvilken aktivitet som ble begått, og hvem som gjorde det. Departementets høringsnotat sier lite eller ingen ting om hvordan slik kobling skal foregå hverken mot nasjonale registre eller internasjonalt samarbeide. Dette er lite betryggende, siden det er nettopp gjennom systemet av alle tilgjengelige kilder at effekten av dette tiltaket vil bli effektuert. Dette er en form for sminking av av den stadig mer inngripende elektroniske overvåkingen som finner sted både nasjonalt og internasjonalt.
- For å omgå IP-logging finnes det kjente teknikker. I høringsnotatet er det klart at departementet er kjent både med bruk av VPN-forbindelser av forskjellig slag, og bruk av anti-overvåkningsteknologi som «TOR»-rutere.
- «Vel», vil en overvåkningsvennlig lovgiver kunne tenke, «da er det bare å introdusere begrensninger på bruk av VPN- og TOR-teknologi». Det er mange land som allerede har introdusert slike begrensninger (Hviterussland, Irak, Iran, Uganda, Kina, Russland, Tyrkia m.fl.[10]).
- Da vil en fortsatt ha sterk kryptering igjen som en barriere for innsyn, så den neste tanken vil da bli «.. og dessuten må vi introdusere sterkere begrensninger på bruk av sterk kryptografi, gjerne med tvungen nøkkelutlevering». Dette har vært foreslått mange ganger. Mest kjent var kanskje «Clipper chip»-forslaget i USA [11], men så sent som i 2020 ble et forslag luftet i EU-kommisjonen om noe tilsvarende [12]. Dette er en upraktisk og udemokratisk idé, men det er ikke en idé som er definitivt død. Den må slås ned med jevne mellomrom.
- ... og bare for å være sikker: «og dessuten bør vi vel også kreve å ha å programvare for dataavlesning installert på alle datamaskiner, slik at vi kan få se hva som virkelig foregår dersom vi virkelig mener at vi trenger det, tenk på barna, og terroristene.»

Når det siste steget er nådd, vil det ikke være noen som har noe sted borgere i et moderne internettbasert samfunn kan ha et beskyttet privatliv. Siden nær alle aspekter av livet som foregår via nettet vil være åpent tilgjengelig for de i politi og etterretning som har de riktige tilgangene. Denne type makt bør ganske enkelt ingen ha.

Grunnen til at det er lett å bli oppgitt, og litt paranoid, er at det ikke på noe sted i listen over er noen klar, prinsipiell og uoverstigelig grense som blir tråkket over. I hvert ledd er det politi og etterretnings legitime behov for å ha verktøy for å beskytte statens interesser som gjør at man går ett skritt til i retning av det totale overvåkningssamfunn. I den angjeldende sak, lagring av IP-adresser, fremstilles det som om det man ber om er helt nødvendig, og at eventuelle motforestillinger er godt tatt i vare. Dette til tross for at man kun i begrenset grad har problematisert systemene informasjonen skal settes inn i, hvilken konkret nytte man vil få, hvordan nytten skal evalueres, og ikke minst, hvorfor er dette, og ikke et mindre eller et større steg hva man virkelig trenger? Spesielt det siste er viktig, det er lett å bli dratt inn i argumenter av typen «tåler du denne, så tåler du litt til». Trusselen blir større fordi argumentene som brukes er lite presise, lite etterprøvbare, og hverken sier klart fra i hvilken retning man er på vei, eller hvor man skal si «så langt, men ikke lenger».

IP-adresser i nettverk som nytter NAT-løsninger

Høringsforslaget beskriver NAT-baserte løsninger slik de var mange år tilbake, og i en slik kontekst ville det vært mulig å lagre brukerens IP-adresser uten videre inngripende metoder.

Med mobile enheter som benytter trådløs kommunikasjon over IP har det vokst fram komplekse NAT-løsninger, Carrier Grade NAT (CGN), fram til i dag hvor flere enn 90% av alle mobilnettleverandører benytter slike løsninger, mens litt færre installasjoner i husholdninger er knyttet mot slike løsninger.

Avstanden fra en bruker til nettleverandørens ytterkant, hvor den eksterne IP-adressen tildeles via CGN kan være – og er gjerne – flere «hopp». To til fire NAT-bokser passeres underveis, men opptil 12-15 er målt i større mobilnett. Mellom den eksterne (offisielle) adressen og brukeren kan IP-adresse endres flere ganger. Både brukerens enhet (source) og endepunktet som brukeren aksesserer (destination) blir en del av adresseringen for å få til dette, sammen med portnumre og nøyaktig tidspunkt for transaksjonen.

I tillegg til dette, så nyttes NAT-baserte løsninger internt i operatørens eget nett. Kompleksiteten er høy og systemene fremstår ofte som uoversiktlige.

I praksis betyr dette at en IP-adresse ikke lengre identifiserer et endepunkt, slik at et høyt volum med tilleggsdata kreves for å sammenstille en IP-adresse med et endepunkt.

Når en har disse dataene lagret som foreslått kan en mappe IP-adresser mot endepunkter og derfra finne ut av hvem som har vært i kontakt med ethvert nettsted i løpet av de siste 6 til 12 måneder.

Metadata (IP-adresse til og fra, dato/tidsstempel, portnummer) er kun en midlertidig identifikasjon, og da med gyldighet for det korte tidsrommet transaksjonen varer. Om ikke dette er nok, så kan en transaksjon skifte IP-adresse mens transaksjonen pågår. Forklaringen ovenfor er sterkt forenklet.

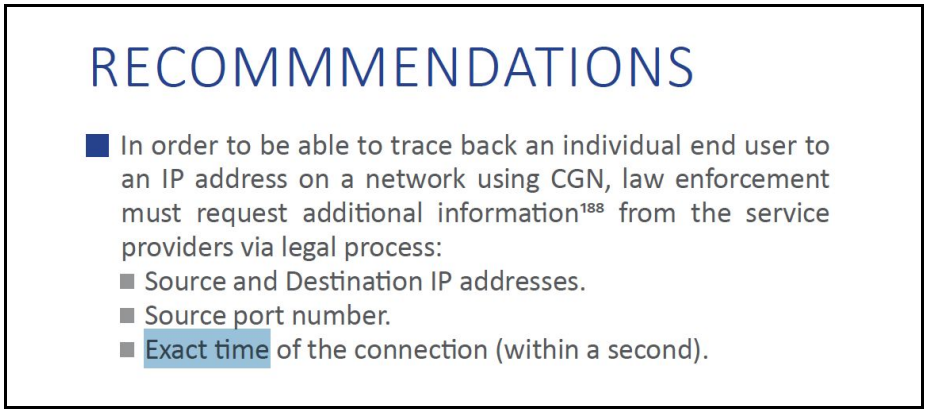
CGN-løsninger vil ofte klassifisere trafikk i forhold til innhold, og vil dermed bruke om enkeltbrukere bruker nettet til å se på avisen, TV, fotball, porno eller noe annet. Dette er informasjon som både brukes internt til trafikkplanlegging, og i noen tilfeller (dog ikke i Norge, såvidt EFN er kjent med) til å prise trafikk til forskjellige typer innhold forskjellig.

Kompleksiteten vanskeliggjør teknisk feilsøking i slike nett.
Og vanskeliggjør også politiets arbeide ved kriminalitet da tusener kan dele samme IP-adressering. Internets Security and Stability Advisory Committee (SSAC) publiserte derfor en egen rapport om endringene relatert til semantikken for IP-adresser [14].

Analogien Regjeringen bruker ved å sammenligne IP-adresse med et telefonnummer eller en postadresse for brevforsendelser i kontekst av dette høringsforslaget hadde relevans 10 år tilbake, men er direkte feil her.

Europol har tatt opp problematikken flere ganger, og i sin trusselvurdering for 2015-2016 (Ref. IOCTA 2016) [3] skriver de, i tråd med rapporten fra SSAC, at for å kunne spore IP-adresser fra Carrier Grade NAT løsninger, trenger de både avsenders og mottakers IP-adresse, samt portnummer og eksakt tidspunkt for transaksjonen.

Videre skriver Europol at ECJ's rettsavgjørelse vedrørende Datalagringsdirektivet blokkerer for dette. Europol lobber også Det Europeiske Råd, og ber muliggjøring av å spore transaksjoner via lagring av «Source and Destination IP addresses; Exact time of the connection (within a second); Source port number».



Fra Interpols trusselvurdering 015-2016 (Ref. IOCTA 2016) [3, side 58]

Hva Regjeringen har lagt på høring her, er det samme som EUROPOL skriver, dvs. lagre alt internettbrukerne (source) gjør i form av hvilke nettsteder og tjenester de benytter/leser (destinasjon for IP-adresse), med eksakte tidspunkt. Ved mobilnettets NAT-baserte løsninger holder det ikke å lagre eksternt tildelt IP-nummer og portnummer (og tidspunkt). En trenger også destinasjonsadressen for å kunne knytte hendelser sammen.

En leverandør må også lagre alt dette for å kunne knytte en bruker til en gitt transaksjon på et gitt tidspunkt. Dette kan også være såpass komplisert at det ikke er gitt at nettleverandøren vil kunne gjøre dette for alle transaksjoner. Mellom brukeren og

operatørens nettgrense utad, hvor brukeren tildeles IP-nummeret som kan rutes på det offentlige nettet er (eller kan være) flere nivåer NAT løsninger, applikasjons-gateways, proxy'er og brannvegger. Alle disse bidrar til kompleksiteten, og med ytterligere lagring av metadata om IP-adresse skal kunne knyttes mot en unik bruker.

Carrier Grade NAT løsninger er mer komplekse enn det gis uttrykk for her, og hvor lagring av IP-adresser i realiteten blir lagring av data om kommunikasjonen, dvs. lagring av metadata.

Departementet skriver også selv at

«Formålet med lagringen vil nettopp være å kunne knytte opplysningene til annen informasjon, slik som hvilken nettaktivitet en IP-adresse er benyttet til.»

Lovforslag er diffust om hva som foreslås lagret.

Departementet henviser til at det er «en positiv forpliktelse til å muliggjøre etterforskning av lovbrudd», jf. «*K.U mot Finland».* Saken det henvises til er relatert til at nettoperatør kjenner en gitt abonnements IP-adresse, og saken har ikke relevans for hva dette høringsforslaget foreslår.

Det er heller ikke riktig slik departementet skriver, at «*koblingen mellom en IP-adresse og abonnent vil i seg selv sjelden muliggjøre en entydig identifikasjon av en konkret bruker.*»

For et mobilabonnement er det høyst *sannsynlig* at abonnementets enhet kan knyttes til en konkret bruker.

Videre mener departementet at «*IP-adresser har tradisjonelt vært ansett som mindre beskyttelsesverdige*».

Dette utsagnet kommer i konflikt med EU's Data Protection Directive 95/46/EC, artikkel 2(a), [7] og også GDPR (art.4) [8], samt fra Article 29 Data Protection Working Party. [9] IP-adresse er ansett som «personal data». Der foreligger også dom fra CJEU om at også dynamisk IP-adresse kan ansees som personlig data[13].

I tillegg, den IP-lagringen som her foreslås vil også inneholde abonnentens/brukerens navn, adresse, osv.

Det hevdes at Skype og iMessage tar over tradisjonell telefoni og SMS. Disse løsningene har vært i bruk henholdsvis nesten 20 og 10 år og er bundet mot en gitt (identifiserbar) brukerkonto. Ved kriminalitet så kan data om brukerens konto opplysninger hentes ut. Den lagringen som foreslås her vil selvsagt vise at brukeren har nyttet Skype (eller hvilket som helst annet nettsted/tjeneste) på et gitt tidspunkt.

På den ene siden presiserer departementet at det foreslås at IP-adresse og portnummer skal lagres, og presiserer at *kun* dette skal lagres.

På den annen side fremgår det klart at departementet er oppmerksom på at dette vil kreve lagring av en god del mere, som forklart ovenfor under punkt 1.

Under «Hvem skal lagre» (høringsdokumentet side 28) samt selve lovforslaget fremkommer det at også VPN-tilbydere vil pålegges lagring av brukernes identifikasjon og IP-adresser aksessert.

På samme side (side 28) skriver departementet:

«Det kan samtidig ikke helt utelukkes at det ved bruk av NAT i enkelte tekniske løsninger vil være nødvendig å lagre noe mer informasjon for å identifisere abonnenter, som også sier noen om destinasjon».

Under lovforslaget gis hjemmel for ytterligere regulering i forskrift: Dersom det viser seg å bli behov for det, kan det blant annet gis bestemmelser som presiseres nærmere hvilke opplysninger som er omfattet av lagringsplikten.

I realiteten foreslås det her å lagre hva landets nettbrukere aksesserer og på hvilket tidspunkt.

Det foreslås i tillegg at myndigheter skal kunne hente ut opplysninger om all nettbruk fra en gitt, identifisert bruker, over et lengre tidsrom.

*Med de analyseverktøy som foreligger i dag så får en fort assosiasjoner til en modernisert utgave av Datalagringsdirektivet, eller en litt nedskalert «Tilrettelagt Innhenting», og er svært inngripende***.**

Formålet er ikke klart definert eller avgrenset.

Formålet med forslaget oppgis å være kriminalitetsbekjempelse så vel som sivile saker, er ikke avgrenset eller klart definert og kan vanskelig defineres som strikt nødvendig i et demokratisk samfunn.

Departementet skriver at en sentral del med lovforslaget er å legge til rette for at politiet skal kunne innhente IP-informasjon i de sakene de faglig sett har behov for det i kampen mot alvorlig kriminalitet. Videre skriver de at politiet har opplyst at de forventer at antall anmodninger om uthenting av IP-informasjon vil øke betydelig ved innføring av lovforslaget, og at en forutsetning for oppfyllelse av formålet med lovforslaget at politiet kan innhente IP-informasjon i flere saker enn i dag.

Ingen krav til hvor data kan lagres eller hvordan brukes.

Domstolkontroll kreves ikke da det er foreslått selvbetjening av lagrede data med henvisning til at utlevering av abonnementsopplysninger til påtalemyndigheten eller politiet krever etter gjeldende rett ikke rettens kjennelse eller at Nasjonal kommunikasjonsmyndighet fritar tilbyder fra taushetsplikten.

Departementet mener at lagrede data ikke representerer noen større inngrep i den private sfære.

Det stilles heller ingen spesiell krav til lagring eller geografisk sted for lagring av datamengden utover hva som antas er ivaretatt allerede fra nett- og tjenestetilbyder.
Det er gjennomgående i forslaget at departementet ikke vurderer vernet om personlig kommunikasjon høyt.

EFN stiller seg svært skeptisk til alle sider av departementets vurdering på dette punktet.

FN’s bærekraftsmål

Departementet refererer på høringsnotatets side en til FNs bærekraftsmål (16.2) om å «Stanse overgrep, utnytting, menneskehandel og alle former for vold og tortur mot barn», dette brukes av departementet som et argument for å introdusere utvidet lagring av IP-adresser. Vi vil imidlertid også trekke frem noen flere av FNs bærekraftsmål [4] og hvordan disse påvirkes av forslaget:

- 13.2: *«Innarbeide tiltak mot klimaendringer i politikk, strategier og planlegging på nasjonalt nivå*»: Det blir i departementets forslag ikke problematisert i hvilken grad overvåkningstjenestene vil forbruke energi. Datasentre er estimert til å bruke 20% (opp til 25%) av verdens energiforbruk innen 5 år [5]. En må ha et bevisst forhold til datamengder en ønskes lagres, og ikke lagre mer data enn det en strengt tatt trenger. Den foreslåtte loven vil kreve lagring av enorme mengder data, ha store økonomiske kostnader, er inngripende i personvernet - og da er ikke klima kostnadene beregnet eller inkludert.
  Det er estimert at ekstra datamengde pr. bruker pr. måned vil være 150MB. For en million abonnenter utgjør dette en volum i størrelsesorden 150 terabyte pr. måned. [15]. Et klimaregnskap for overvåkningstiltak bør i dag være en naturlig del av departementets fremstilling, men vi noterer oss at dette er et helt oversett perspektiv i høringsnotatet.

- 16.3: *«Fremme rettsstaten nasjonalt og internasjonalt, og sikre likhet for loven, rettssikkerhet og rettsvern for alle*» samt 5.b: «*Styrke bruken av muliggjørende teknologi, særing informasjons- og kommunikasjonsteknologi, for å styrke kvinners stilling i samfunnet*». Sårbare og forfulgte grupper har gjennom Internett mulighet til å kommunisere med hverandre, og med grupper som kan hjelpe dem. Slik kommunikasjon, det være seg med journalister, menneskerettighetsorganisasjoner familie og andre, er i mange regimer i verden underlagt strenge restriksjoner og overvåkning. Det er derfor rimelig av de som sitter i begge ender av slik kommunikasjon, også de som er bosatt og opererer fra land med god rettslig beskyttelse, beskytter sin kommunikasjon med virtuelle private nett, og annen anti-overvåknings beskyttelse slik som nettverksteknologien «TOR» [6]. Problemet i forhold til lagring av IP-adresser er at nøyaktig den samme teknologien som kan brukes for å fremme rettighetene til forfulgte og undertrykte, også kan brukes av kriminelle for å unngå overvåkning. Det er altså ikke mulig å la Internett bli brukt til å fremme 16.3 og 5b i bærekraftsmålene samtidig som man også gjør det mulig å omgå tiltak for å stoppe 16.2. Dette er et paradoks, men det er reelt og vil ikke forsvinne av å ikke snakke om det.

Prinsipielt sett ser ikke EFN at en kan fremme en menneskerettighet, her representert ved bærekraftsmål, ved å underminere en annen fundamental menneskerettighet. Departementets forslag forsøker ikke å balansere støtte til de forskjellig bærekraftsmålene mot hverandre, fremstår derfor som ubalansert, de tiltak som foreslås er ute av proporsjoner i forhold til den nytte det vil gi både med hensyn til klima, miljø og til menneskerettigheter.

Gode alternativer

Carrier Grade Nat (CGN) bringer mange problemer. Politietterforskere, tekniske fagpersoner og relevante organisasjoner er enige i at CGN er svært problematisk. Kompleksiteten vanskeliggjør teknisk feilsøking, IP-adresser er irregulære, implementasjoner av disse «nøstede» NAT-løsningene følger ikke internettstandarder (gitt fra IETF), geografiske lokasjonsdata mistes, og skytjenester forsterker her problematikken.

CGN er heller ikke bra for forbrukerne. I praksis medfører slike løsninger at forbrukeren/kunden ikke får fullverdig internett-tjeneste. Der er flere internet-tjenester som ikke kan fungere ved nestede NAT-løsninger, da de forskjellige internett protokoller har varierende krav for å etablere start av en kommunikasjons-sesjon.

IP-adresser som tildeles via omtalte løsninger vil også, dessverre medføre at tilfeldige brukere får tildelt IP-adresser som er heftet med kriminell atferd, eventuelt også deler samme IP-adresse med en kriminell.

Kostnadene ved dette lovforslaget er svært store, både for utvikling, drift og vedlikehold. Sannsynligheten for at ikke alle transaksjoner (bruk av IP-adresser) vil kunne kobles mot en bestemt bruker/abonnenter og store grunnet kompleksiteten i løsningene.
Det er heller ingen grunn til å tro at dette vil bli enklere videre framover.

Både sikkerhet og personvern reguleres ved fysiske implementasjoner som oppfyller respektive tekniske krav, kombinert med lovregulering. Det hadde vært ønskelig at nettoperatører gis insentiver for å migrere til ny teknologi, dvs. IPv6. Om ikke så skjer, og slike løsninger som vi har sett med nøstede NATs og CGNAT får fortsette sine egne veier, vil det skade politiets muligheter til etterforskning, så vel som for teknisk feilsøking i nett men også for både for oppgradering til ny teknologi, løsninger og innovasjon på veien fremover.

I et klimaperspektiv bør vi også gjøre dette. Uten incitamenter og et mildt press fra myndigheter på nettleverandørene vil vi måtte leve med IPv4's nåværende surrogater for IP-adresser. Dette er ikke tjenlig for noen parter.

Eksempelvis kan nettleverandører pålegges at det skjer en prosentvis økning av IPv6 årlig slik at målet nås innen forutsigbar tid. Vi må riktig nok leve med både IPv4 og IPv6 mange år fremover, men en er nødt til å starte denne prosessen nå.

Lovforslaget indikerer at høye millionbeløp nyttes til lagring av brukerdata, som i stedet kan benyttes til oppgradering av infrastruktur.

Konklusjon og tilrådinger

Vi ser ikke at departementets forslag er vesensforskjellig fra fra det tidligere vedtatte Datalagringsdirektivet. Det har dessuten foregått en rivende teknisk utvikling siden Datalagringsdirektivet ble vedtatt. Internett-kommunikasjon har siden den tid blitt ennå dypere integrert i alle deler av samfunnet. Vi tror ikke det er en god ide å utvide pliktmessig lagring av IP adresser, eventuelt m.m. ihht forskrifter. Departementets forslag er i så måte for diffust. Men selv der det ikke er diffust kan ikke vi se at det vil kunne være i henhold til gjeldende EU rett mht personvern.

Vår primære tilrådning er derfor at dette forslaget ikke realitetsbehandles, og at dagens ordning med lagring av IP data kun til forretningsmessig betinget bruk videreføres.

Videre tilrår vi at politiets ressurser til etterforskning av online-kriminalitet styrkes, slik at man bl.a. kan bruke de dataressurser som er er tilgjengelige i dag mer effektivt, og dessuten pålegge ISPer over en viss størrelse å tilby IPV6 til sluttbruker.

Med vennlig hilsen
ELEKTRONISK FORPOST NORGE

Bjørn Remseth
Nestleder

Brit Lysaa
Utvalgsmedlem for høringen

Referanser

[1] Regjeringens høringsnotat om endringer i ekomloven (20/3645-1)
https://www.regjeringen.no/no/dokumenter/horing---endringer-i-ekomloven/id2766348/

[2] https://svar.regjeringen.no/nb/registrer_horingsuttalelse/H2766348/

[3] THE INTERNET ORGANISED CRIME THREAT ASSESSMENT (IOCTA) 2016
https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016

[4] FNs bærekraftsmål.
https://www.fn.no/om-fn/fns-baerekraftsmaal/fred-rettferdighet-og-velfungerende-institusjoner

[5] "Energy consumption and emission mitigation prediction based on data center traffic and PUE for global data centers" by Yanan Liua, Xiaoxia Wei, JinyuXiao , Zhijie Liu, Yang Xua, Yun Tiana in Global Energy Interconnection Volume 3, Issue 3, June 2020, Pages 272-282.
https://www.sciencedirect.com/science/article/pii/S2096511720300761

[6] torproject.org

[7] EU's Data Protection Directive 95/46/EC.
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31995L0046

[8] "REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)"
https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679

[9] EU commission "Article 29 Working Party" https://ec.europa.eu/newsroom/article29/news-overview.cfm

[10] ProtonVPNs liste over land som forbyr eller ønsker å forby bruk av VPN teknologi
https://protonvpn.com/blog/are-vpns-illegal/

[11] "The clipper chip" https://epic.org/crypto/clipper/

[12] "European Commission Does Not Support Backdoors To Encrypted Communications"

https://www.medianama.com/2020/09/223-no-backdoors-for-encrypted-communications-says-european-commission/

[13] Court confirms that IP addresses are personal data in some cases. OCT 31, 2016. By Dr. Martin Munz Tim Hickman

https://www.whitecase.com/publications/alert/court-confirms-ip-addresses-are-personal-data-some-cases

[14] SSAC Advisory on the Changing Natureof IPv4 Address Semantics
https://www.icann.org/en/system/files/files/sac-079-en.pdf

[15] IETF Approaches to Address the Availability of Information in Criminal Investigations Involving Large-Scale IP Address Sharing Technologies - draft