ØKOKRIM

Kommunal- og moderniseringsdepartementet

Deres referanse:	Vår referanse:	Dato:
20/3645-1		11.01.2021

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

Det vises til høringsbrev datert 9. oktober 2020 fra Kommunal- og moderniseringsdepartementet om forslag til endringer i lov 4. juli 2003 nr. 83 om elektronisk kommunikasjon (ekomloven).

Sikring av digitale spor er stadig viktigere for en effektiv kriminalitetsbekjempelse for politi- og påtalemyndighet. ØKOKRIM slutter seg derfor til departementets argumentasjon om behovet for å lovregulere lagringsplikt for IP-adresser og portnummer. ØKOKRIM vil i sitt høringssvar vektlegge argumentasjon knyttet til lagringstid for IP-adresser/abonnementsinformasjon og strafferammekrav for utlevering av identifiserbar informasjon knyttet til sluttbrukeren.

ØKOKRIM har nasjonalt ansvar for forebygging og bekjempelse av miljø- og økonomisk kriminalitet i Norge jf. påtaleinstruksens kapittel 35, og vil derfor vektlegge argumentasjon med utgangspunkt i disse kriminalitetsområdene.

7.1 - Bør det innføres plikt til IP-lagring?

Forslaget om lagring av IP-adresser reiser prinsipielle spørsmål i spennet mellom effektiv kriminalitetsbekjempelse, ytringsfrihet og retten til privatliv. ØKOKRIM mener høringsnotatet fra departementet gir en grundig, nødvendig og god drøftelse av dette.

ØKOKRIM mener lagring av IP-adresser totalt sett innebærer et mindre inngrep i person- og kommunikasjonsvernet til den enkelte borger all den tid slik lagring ikke innbefatter metadata. Ulemper i form av nedkjølingseffekt og forskyvningsmekanismer er etter ØKOKRIM sitt syn begrenset sammenlignet med nytteverdien lagring vil ha for å ivareta offentlig trygghet, forebygging av uorden eller kriminalitet og beskyttelse av andres rettigheter og friheter. Vi viser her til sammenlignbare land som Sverige, Danmark, Finland og Island, hvor lagringsplikt allerede er innført.

Inngrepets begrensede omfang, slik det er angitt i høringsnotatet, kan til en viss grad sammenlignes med andre regulative krav til for eksempel registreringsplikt av

Postadresse
Postboks 2096 Vika
NO-0125 OSLO

Besøksadresse
C.J. Hambros plass 2 C
NO-0164 OSLO

Telefon/Telefaks
(+47) 23 29 10 00
(+47) 23 29 10 01

Org.nr.: 874 761 532
post.okokrim@politiet.no
www.okokrim.no

motorkjøretøy eller teletilbydernes plikt til å lagre og utlevere abonnementsinformasjon om kunden ved kjøp av simkort til mobiltelefoni. En annen parallell mellom den fysiske og digitale verden er den forpliktelsen borgerne har etter straffelovens § 162 om identifikasjonsplikt overfor myndighetene når det foreligger tjenestemessig behov for dette.

ØKOKRIM vil også fremheve at forslaget om lagringsplikt er relevant i en rettsikkerhetskontekst. Lagring av identifikatorer vil i en etterforskning kunne bidra til å klarlegge uskyld jf. politiets objektivitetsplikt etter strpl. § 226 3. ledd.

7.1.2 - Behovet for opplysninger om IP-adresser i kriminalitetsbekjempelsen

ØKOKRIM har som øvrige politi- og kontrollmyndigheter erfart hvordan den digitale utviklingen har påvirket og endret modus innenfor de ulike kriminalitetsområdene. Digitale bevis gjennom speilkopi av databeslag til ulike former for digital kommunikasjon er i dag elementer i de aller fleste saker som ØKOKRIM har befatning med.

ØKOKRIM har de senere årene beskrevet utfordringer knyttet til digitaliseringen av kriminaliteten, se blant annet trusselvurdering fra 2018[1] og 2020.[2] Her fremheves det hvordan kriminelle aktører utnytter nye digitale betalingstjenester, bruk av digital valuta, og bankidentifikasjonssystemer (bank-id) som verktøy for å begå kriminalitet.

Økokrim har bidratt innen etterretning, etterforskning og forebygging i flere saker hvor nordmenn er domfelt for kjøp av overgrepsmaterialer, og hvor kjøp har vært kamuflert ved bruk av kryptovaluta.

ØKOKRIM har i forbindelse med Covid-19-pandemien prioritert tiltak rettet mot misbruk av offentlige støtteordninger. I ØKOKRIMs trusselvurdering for 2020 omtales denne formen for kriminalitet som godt organisert, hvor spesielt utnyttelse av lønnskompensasjonsordningen ved permitteringer blir misbrukt. Pengene flyttes raskt mellom flere personer og bankkonti, det benyttes stråmenn og det er utstrakt bruk av utlånt og misbrukt digital ID. Aktørene har også omfattende kontakt med kjente kriminelle. Hvert tilfelle omfatter bedrageri mot NAV i størrelsesorden fra kr 500.000 - 5.000.000. Eksempelet illustrerer hvordan bedragerier rettet mot det offentlige utnytter raske digitale transaksjoner mellom ulike aktører, noe som igjen innebærer et sterkt behov for å kunne identifisere aktørene gjennom IP-sporing.

Et eksempel på utfordringer knyttet til manglende IP -lagring er Hedmark Tingretts dom 20-082850MED-HEDM fra 2020 som gjaldt bedragerier og bedrageriforsøk begått overfor forskjellige banker og kredittinstitusjoner i perioden fra april 2017 til november 2018. Ved bruk av uriktige opplysninger og falske dokumenter er det søkt om og innvilget lån og kreditt i en rekke personers navn ved bruk av blant annet forfalskede bank – id. De fullbyrdede bedrageriene utgjorde ca. 22 millioner kroner, og forsøk på

[1] https://www.okokrim.no/okokrims-trusselvurdering-2018.6123197-411472.html
[2] https://www.okokrim.no/trusselvurdering-2020.6304950-411472.html

bedragerier rundt 40 millioner kroner. I dommen (s. 96) vises det til hvordan manglende lagrede data om IP – adresser knyttet til abonnement vanskeliggjorde etterforskningen.

7.3 – Utformingen av regler om lagringsplikten

Det må ved innføring av lagrinsplikt stilles krav til sikker lagring og øvrig behandling av personopplysningene på lik linje med de krav og den praksis som fremgår i f.eks. ekomloven og datalagringsforskriften. Videre må en lovendring sørge for at lagringsplikten blir tilstrekkelig teknologinøytral, slik at formålet om en identifisering av abonnenten blir ivaretatt til tross for fremtidige teknologiske endringer og nye løsninger som strekker seg utover IP-adresser og portnummer. I tillegg må data tilrettelegges slik at dette skjer sentralisert, sømløst, og i et ensartet format ved utlevering til politiet.

7.4 – Lagringstid

Det er en grunnleggende kvalitetskomponent innen etterforskning og iretteføring av straffesaker at saksbehandlingstiden skal være tilstrekkelig effektiv (adekvat saksbehandlingstid). ØKOKRIMs ulike prosjekter innen etterforskning, forebygging og etterretning er imidlertid kompliserte og relativt tidkrevende. Saksbehandlingstiden ved ØKOKRIM innen etterforskning fra saksinntak til påtalevedtak har de siste seks årene variert fra 216 – 560 dager (2014 – 2019).

ØKOKRIM mottar også anmeldelser fra ulike tilsyns- og kontrollorgan, blant annet Finanstilsynet, Skattedirektoratet, NAV, Næringsmiddeltilsyn, Tollvesen mv. Dette er saker som ytterligere pådrar seg saksbehandlingstid forut for ØKOKRIMs saksinntak.

ØKOKRIMs prosjekter har ofte forgreininger til utlandet, noe som medfører internasjonalt judisielt samarbeid i form av rettsanmodninger. Dette kan være til dels tidkrevende prosesser avhengig av hvilke land det samarbeides med.

ØKOKRIM mener derfor det vil være strengt nødvendig at lagringstid av IP – adresser, knyttet til identifiserbar abonnentinformasjon, settes til 12 måneder for å ivareta hensynet til kompleksiteten i de saker som etterforskes og forebygges ved ØKOKRIM.

7.5.1 – Strafferammekrav/forebygging av kriminalitet

I høringsnotatet vises det til rettspraksis fra EU-domstolen som angir krav om at det skal foreligge *alvorlig kriminalitet* for å kunne utlevere IP-adresser. De sakene som ØKOKRIM har befatning med vil i stor grad ha strafferamme fra tre år og oppover, slik at en terskeldiskusjon på mellom 1- 2 år har mindre betydning for ØKOKRIM sine saker.

ØKOKRIM er imidlertid av den oppfatning at strafferammekravet for innhenting av abonnementsinformasjon knyttet til IP-adresser bør legges til mistanke om lovbrudd

som kan medføre frihetsstraff, alstå 6 måneder. Til sammenligning er terskelkravet i strpl. § 192 om ransaking mistanke om frihetsstraff. Innhentning av identifikatorer knyttet til IP-adresser er etter ØKOKRIM sin vurdering et klart mindre inngrep enn eksempelvis husransakning. ØKOKRIM mener også at en differensiering, ut fra lovbruddskategorier, vil være uhensiktsmessig og komplisere utformingen av loven unødvendig.

I høringsnotatet diskuteres eventuelt grunnlag for å kunne benytte lagrede lP-data også innen forebygging av kriminalitet. Det legges til grunn at departementet med forebygging her mener polisiær virksomhet utenfor etterforskningsbegrepets formål jf. strpl. § 226.

Norge har gjennom EUs fjerde hvitvaskingsdirektiv klare forpliktelser til å forebygge og bekjempe hvitvasking og terrorfinansiering, regulert i hvitvaskingsloven. Dette arbeidet har i større grad en forebyggende karakter, ved at det nødvendigvis ikke ender i anmeldelse, etterforskning og iretteføring for domstolen.

Norges Financial Intelligence Unit (FIU) som er lokalisert ved ØKOKRIM mottar jevnlig forespørsler fra andre land om abonnementsinformasjon knyttet til IP-adresser. Det er derfor en svakhet at norske myndigheter i liten grad er i stand til å svare ut slike forespørsler jf. våre internasjonale forpliktelser knyttet til EUs hvitvaskingsdirektiv.

I Nasjonal Risikovurdering, hvitvasking og terrorfinansiering i Norge (Justisdepartementet, 2018 s. 69) er utfordringene knyttet til manglende lagring av IP-adresser og abonnement problematisert med henvisning til de samme internasjonale forpliktelsene. Konkrete eksempler på dette kan typisk være hvordan rapporteringspliktige foretak, etter hvitvaskingsloven, melder inn mistenkelige transaksjoner knyttet til IP-adresser, men hvor manglende abonnementsidentifikasjon vanskeliggjør det videre arbeidet.

ØKOKRIM mener derfor at identifiserbar informasjon knyttet til internettbruk gjennom IP-adresser også må tillates benyttet til å forebygge kriminalitet av samme alvorlighetsgrad som angitt for etterforskning. Dette til tross for at formålet med tiltaket ikke omfattes av etterforskningsbegrepet jf. straffeprosesslovens § 226.

Med hilsen

Inge Svae-Grotli
Ass. sjef ØKOKRIM

Torstein Eidet
Politiinspektør

Dokumentet er elektronisk godkjent uten signatur