POLITIET
POLITIDIREKTORATET

Kommunal- og moderniseringsdepartementet
Postboks 8112 Dep
0032 Oslo

NATIONAL POLICE DIRECTORATE

Deres referanse:	Vår referanse:	Sted, Dato
20/3645	20/126210	Oslo, 10.02.2021

HØRINGSSVAR – FORSLAG TIL ENDRINGER I EKOMLOVEN (LAGRING AV IP-ADRESSER MV.)

Vi viser til Kommunal- og moderniseringsdepartementets (KMD) høringsbrev av 9. oktober 2020 med forslag til endringer i ekomloven (lagring av IP-adresser mv.). Høringsfristen er etter avtale med departementet forlenget til 25. januar 2021. Direktoratet beklager at fristen er oversittet.

Politidirektoratet har forelagt høringen for samtlige politidistrikt, Kripos, Økokrim, Politihøgskolen og Politiets utlendingsenhet. Politidirektoratet har mottatt høringssvar fra politidistriktene Sør-Øst, Innlandet, Sør-Vest, Nordland, Øst, Oslo, og Trøndelag, samt fra Kripos, Politihøgskolen, Politiets utlendingsenhet og Økokrim. Økokrim har gitt sitt høringssvar direkte til departementet med kopi til Politidirektoratet. Samtlige høringssvar er vedlagt.

Kort om høringen

Endringsforslaget innebærer at det innføres en plikt for tilbydere av ekomtjenester til å lagre IP-adresser, slik at politiet kan få tilgang til IP-adressene for å forebygge eller etterforske alvorlig kriminalitet. Departementene (KMD og Justis- og beredskapsdepartementet) fremholder i høringsnotatet at endringsforslaget blant annet vil kunne bidra til å forhindre og oppklare nettkriminalitet, og være et viktig virkemiddel for å oppnå FNs bærekraftmål 16.2 om å stanse overgrep, utnytting, menneskehandel og alle former for vold mot og tortur av barn. Departementene ber særskilt om høringsinstansenes syn på hvilket strafferammekrav som bør oppstilles, og hvor lang lagringstiden bør være.

Politidirektoratets merknader

Politidirektoratet kan i det alt vesentlige slutte seg til de vurderinger og forslag som fremmes i departementene i høringsnotatet. Det er også bred støtte til de foreslåtte endringer i de mottatte høringsinnspill fra politietaten.

Lengre lagringstid av abonnementsinformasjon for IP-adresser har vært et savn hos politiet lenge, og en lovfesting i samsvar med forslaget vil medføre en tilpasning til regelverkene til de fleste europeiske land. Det er snakk om relativt små inngrep i personvernet samtidig som endringene vil bidra til en mer effektiv etterforskning av straffbare forhold, en etterforskning som i stadig større grad er rettet mot forhold og aktører på internett eller der sentrale bevis er å finne på nettet.

Politidirektoratet

Post: Postboks 2090 Vika, 0125 Oslo
Besøk: Fridtjof Nansens vei 14/16
Tlf: 23 36 41 00
Faks: 23 36 42 96
E-post: politidirektoratet@politiet.no
Org. nr.: 982 531 950
Giro: 7694.05.02388
www.politi.no

Politidirektoratet vil i det følgende kommentere enkelte forhold i høringen. For øvrig vises det til vedlagte innspill fra underliggende enheter. Politidirektoratet finner grunn til å framheve høringsinnspillet fra Kripos.

Den følgende nummerering er i samsvar med nummereringen i høringsnotatet.

7.1 Bør det innføres plikt til IP-lagring?
Etter Politidirektoratets syn beskriver høringsnotatet punkt 7.1.2 behovet for opplysninger om IP-adresser i kriminalitetsbekjempelsen på en god måte. Politidirektoratet tiltrer departementenes vurdering av at det ikke er tvilsomt at informasjon om IP-adresser vil være et viktig verktøy i kriminalitetsbekjempelsen, og at slike opplysninger dermed vil bidra til å ivareta den enkeltes vern mot kriminalitet. En lagringsplikt vil være viktig for bekjempelsen av all form for kriminalitet hvor internett benyttes til kommunikasjon eller annen aktivitet. Lagring av IP-adresser i inntil 21 dager er ikke tilstrekkelig for å kunne benytte slik informasjon til kriminalitetsbekjempelse i dagens digitaliserte samfunn. I et demokratisk samfunn er ivaretakelse av kommunikasjons- og personvernet åpenbart en grunnleggende verdi, men i tråd med departementenes vurdering kan lagring av IP-adresser ikke innebære et så stort inngrep i disse verdier at det bør hindre politiets mulighet til å nyttiggjøre seg opplysningene ved kriminalitetsbekjempelse. Politidirektoratet viser for øvrig til de innledende vurderinger i høringsinnspillet fra Kripos om disse forhold som tiltres.

7.3 Utformingen av regler om lagringsplikten

7.3.1 Hvem skal lagre?
I høringsnotatet foreslås det en lagringsplikt for alle tilbydere av internett. Kripos påpeker i sitt innspill viktigheten av en lagringsplikt også for tilbydere av private nett som skoler, kommuner, hoteller, flyplasser og lignende. Politidirektoratet tiltrer innspillet fra Kripos.

7.3.2 Hva skal lagres?
I høringsnotatet vurderes ulike tilnærminger ved utforming av reglene for hva som skal lagres. Det vesentlige er at de opplysningene som lagres muliggjør identifisering av sluttbruker. Politidirektoratet støtter tilnærmingen om at det fastsettes en plikt til å lagre de opplysninger som er nødvendig for formålet som er å identifisere abonnenter som gis internettilgang. Kripos foreslår i sitt høringsinnspill at lagringsplikten knyttes opp mot et teknologinøytralt begrep og at en nærmere presisering av hvilke typer data som til enhver tid skal lagres kan bestemmes i forskrift. Videre uttaler Kripos at tildelingstidspunktet for IP-adressen må omfattes av lagringsplikten. Politidirektoratet tiltrer innspillet fra Kripos.

7.3.3 Hvordan og hvor data skal lagres?
Politidirektoratet har ikke særlige innspill til hvor dataene skal lagres. Det avgjørende for politiet er selve tilgangen til dataene. Politiet må vite hvor de kan hente ut data og det må etableres praktisk gode løsninger med kontaktpunkt hos tilbydere, sikker løsning for overføring av data og kontaktpunkt hos politiet. Det er trolig hensiktsmessig med et sentralt kontaktpunkt hos politiet.

7.4 Lagringstid
Det framgår av høringsnotatet at etter departementenes vurdering bør lagringstiden være innenfor det samme spennet som de øvrige nordiske landene, som er ni, ti eller tolv måneder. Politidirektoratet foreslår en lagringstid på tolv måneder, da dette i større grad ivaretar politiets behov. Politidirektoratet spilte inn lagringstid på tolv måneder også da implementering

av datalagringsdirektivet var på høring i 2010. En lagringstid på tolv måneder er også det gjennomgående forslaget i høringsinnspillene fra politietaten. Kripos mener også at lagringstiden bør være tolv måneder og uttaler videre:

> "Behovet som underbygger denne lagringstiden har ikke blitt mindre med tiden som har gått, snarere tvert om. Ofte vil det kreve en omfattende etterforskning for å skaffe til veie informasjon om nettaktivitet. Gjennomgangen av beslaglagte telefoner og datamaskiner tar lang tid og underveis er det behov for å bruke tvangsmidler som ransaking, beslag og utleveringspålegg for å få tilgang til data som kan si noe om vedkommende aktivitet.
>
> Internett er globalt og det vil som regel være behov for rettsanmodninger om utlevering av informasjon fra utenlandske nettsteder. Det kan han nevnes at en rettsanmodning til USA om innhenting av data fra en tilbyder av innholdstjenester vil kunne ta opptil tolv måneder. Selv om dataene som amerikanske tjenestetilbydere har om europeiske brukere skulle bli flyttet til Europa er det grunn til å tro at det vil ta flere måneder for å få ut data gjennom en rettsanmodning. Stadig mer av kommunikasjon i Norge skjer over Internett gjennom utenlandske tjenestetilbydere, noe som gjør at behovet for å hente ut data gjennom rettsanmodninger er økende.
>
> En gjennomgang av mistenktes kommunikasjonsenhet forutsetter at politiet faktisk får tilgang til enheten som skal undersøkes. Avanserte tilgangsløsninger og kryptering blir mer og mer vanlig og det tar ofte lang tid før politiet kan starte på selve gjennomgangen. Også dette underbygger behovet for lagringstid i tolv måneder".

Politidirektorater tiltrer Kripos sine vurderinger.

7.5 Vilkår for utlevering av lagrede opplysninger

7.5.1 Materielle vilkår for utlevering

Etter gjeldende rett er det en vid adgang til utlevering av opplysninger om IP-adresser, og det kreves ikke at den straffbare handlingen er av en viss alvorlighetsgrad. I høringsnotatet stilles det krav om at utlevering skal betinge at det dreier seg om alvorlig kriminalitet. Dette for å iaktta kravet til proporsjonalitet slik det framgår av Grunnloven, Den europeiske menneskerettighetskonvensjon og EØS-retten (kommunikasjonsdirektivet). I høringsnotatet foreslås det at strafferammekravet bør være minst ett eller to års fengsel eventuelt i kombinasjon med særskilte angitte straffebud.

I samsvar med høringsinnspillene fra Politihøgskolen, Økokrim og Kripos, er det Politidirektoratets oppfatning at vilkår for utlevering kan sammenlignes med vilkår for bruk av tvangsmidler. Ved bruk at tvangsmidler kan politiet få tilgang til svært personsensitivt materiale med strafferammekrav som ligger langt under de strafferammekrav som her foreslås. Økokrim uttaler følgende i sitt høringsinnspill:

> "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, altså 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 husransaking. ØKOKRIM mener også at en differensiering, ut fra

> lovbruddskategorier, vil være uhensiktsmessig og komplisere utformingen av loven unødvendig".

Politihøgskolen skriver i sitt høringsinnspill:

> "Innhenting av abonnementsinformasjon vil ikke være å anse som et tvangsmiddel, slik rettsreglene er foreslått innført. Det er likevel fornuftig å se hen til reglene om bruk av tvangsmidler, da opplysningene kan bli brukt som bevis i straffesaker, og det vil her, som ved bruk av tvangsmidler, være en proporsjonalitetsvurdering, selv om den her legges på generelt nivå i lovreguleringen, og ikke i det enkelte særskilte tilfelle. Til sammenligning kreves det, for å foreta en pågripelse, at siktede mistenkes for en handling som kan medføre fengsel i minst seks måneder, mens for å ransake kreves det at man etterforsker et forhold som kan medføre frihetsstraff. Det er urimelig at et slikt mindre inngrep skal kreve et forutgående straffbart forhold av større alvorlighet, selv om det ikke vil foretas en urimelighetsvurdering i den enkelte sak. Terskelen departementet legger til grunn synes høy i forhold til graden av inngrep".

I tråd med de nevnte høringsinnspill mener Politidirektoratet at strafferammekravet bør ligge lavere enn det som er foreslått. Dersom man skulle komme fram til at det er behov for et strafferammekrav, mener direktoratet at kravet bør settes likt med kravet til å foreta en pågripelse, at siktede mistenkes for en handling som kan medføre fengsel i minst seks måneder. Det vil ved strafferammekrav på fengsel i minst seks måneder ikke være behov for å angi særskilte straffebud.

Politidirektoratet tiltrer forslaget om at opplysninger kan utleveres når det er nødvendig for å forebygge en handling av tilsvarende alvorlighet.

Kripos skriver avslutningsvis under 7.5.1 Materielle vilkår for utlevering, at abonnementsinformasjon er viktig for politiets virksomhet utover i forebyggings- eller etterforsknings øyemed. Det er eksempelvis behov innenfor redningsarbeid eller søk etter savnede personer. Kripos skriver at lagring av abonnementsinformasjon av andre grunner vil kunne gå ned i omfang eller opphøre dersom det nå innføres en lagringsplikt, noe som vil kunne gjøre politiets redningsarbeid eller søk etter savnede personer vanskeligere. Politidirektoratet støtter Kripos sitt forslag om at det med denne bakgrunn bør vurderes om det kan innføres en særregel om at uthenting av abonnementsinformasjon lagret etter en ny § 2–8a til bruk i søk og redning. I denne sammenheng vises til politiloven § 27 tredje ledd hvor det heter at:

> "I ulykkes- og katastrofesituasjoner tilligger det politiet å iverksette de tiltak som er nødvendig for å avverge fare og begrense skade. Inntil ansvaret blir overtatt av annen myndighet, skal politiet organisere og koordinere hjelpeinnsatsen."

7.5.3 prosessuelle garantier ved utlevering

Etter gjeldende rett kreves ikke rettens kjennelse eller fritak fra taushetsplikten fra Nkom for utlevering av abonnementsopplysninger til politi og påtalemyndighet. Politidirektoratet støtter vurderingen i høringsnotatet av at gjeldende rett videreføres på dette punktet. Videre støtter Politidirektoratet forslaget om at det ikke er behov for særskilte regler om behandling av innhentede opplysninger da reglene i politiregisterloven med forskrift må anses dekkende.

7.6 Bruk av opplysninger om IP-adresser i sivile saker

Etter tvisteloven § 21-5 plikter enhver å gi forklaring om faktiske forhold og gi tilgang til gjenstander mv. som kan utgjøre bevis i en straffesak med de begrensinger som følger av reglene om bevisforbud og bevisfritak i kapittel 22 og andre bevisregler i tvisteloven. Politidirektoratet støtter vurderingen i høringsnotatet om at gjeldende rett bør videreføres selv om innføring av en plikt til å lagre IP-adresser vil innebære lengre lagring som igjen kan medføre at IP-adresser i større grad vil kunne føres som bevis.

10 Kostnadsfordelingsmodell

I høringsnotatet er det lagt frem en modell med ulike alternativer for hvordan kostnadene skal beregnes og fordeles mellom tilbydere og myndighetene. I alle modellene er kostnadene delt i tre; investeringskostnader, faste driftskostnader og uthentingskostander. I alle modellene er det lagt til grunn at staten skal dekke uthentingskostnadene, og modellene skiller for øvrig på hvor mye, om noe, staten skal dekke av investerings- og eller driftskostnader. Høringsnotatet viser til at siden formålet med forslaget er kriminalitetsbekjempelse, kan ikke tilbydere forventes å dekke alle kostnadene. Samtidig vektlegges det at modellen skal ivareta konkurransen i ekommarkedet slik at modeller understøtter samfunnsøkonomisk kostnadseffektivitet.

Når det gjelder kostnadsfordelingsmodell uttaler Kripos blant annet følgende:

> "Kripos' klare utgangspunktet er at kostnader knyttet til lagring, herunder investering i og drift av løsninger, må dekkes av tilbyderne selv. Kriminalitetsbekjempelse er et sentralt samfunnsmessig hensyn, og staten bør som er helt klare utgangspunktet kunne pålegge næringer tilretteleggingskrav uten kompensasjon. Kripos kan ikke se at dette tilfellet skiller seg nevneverdig fra for eksempel situasjonen for finansnæringer, som selv er pålagt å dekke kostnadene knyttet til hvitvaskingsregisteret. En utvikling i retning av staten skal måtte betale virksomheter for å legge til rette for ivaretakelsen av grunnleggende samfunnsmessig behov og tjenester, er etter vår oppfatning klart uheldig".

Politidirektoratet tiltrer Kripos sin vurdering.

Politidirektoratet vurderer som Kripos at det er utfordrende å skille mellom investeringskostnader og driftskostnader. Kripos trekker som eksempel fram om det vil bli vurdert som drift eller investering dersom man inngår leasingavtale istedenfor innkjøp av serverpark. Direktoratet mener som Kripos at dersom det velges en løsning hvor staten skal dekke annet enn rene uthentingskostnader, bør man gå for en modell der det ikke skilles mellom investerings- og driftskostnader, jf. modell E. Videre er det direktoratets oppfatning at en fast fordelingsnøkkel mellom tilbyderne blir mest riktig. Det store antallet tilbydere tilsier at individuelle refusjonsavtaler vil være ressurskrevende å drifte.

Kripos peker i sitt innspill på at uthentingskostnader bør begrenses til å gjelde rene kostnader med å hente ut lagrede data og overføre disse til politiet. Videre uttaler Kripos at valget av kostnadsfordelingsmodell ikke må få konsekvenser for om politiet faktisk velger å innhente data, og lage utfordringer for de innarbeidede ordninger som gjelder for innhenting av trafikkdata og tilrettelegging for kommunikasjonskontroll. Politidirektoratet tiltrer Kripos sine vurderinger.

11 Økonomiske og administrative konsekvenser

Dagens praksis er at kompensasjon for utlevering av IP-informasjon avtales mellom politiet og den enkelte tilbyder. Enkelte tilbyr dette i dag gratis mens det for øvrig er stor variasjon i stykkpris (mellom 250 og 1 250 kroner). Gitt en gjennomsnittskostnad på 500 kroner og Kripos sitt estimat for antall anmodninger som ville vært sendt i dag dersom lagringsplikten var innført, er merkostnaden for politiet anslått til om lag 40 millioner kroner årlig. Det forventes at behovet vil vokse, og at merbehovet derfor vil være høyere fremover i tid, gitt at politiet anmoder om IP-informasjon når de faglig sett har behov for det.

Etter Politidirektoratets vurdering vil det foreliggende forslaget innebære betydelige økte utgifter for politiet knyttet til både uthenting, mottak, dekoding og lagring av data fra tilbydere. En videreføring av dagens modell der politiet dekker uthentingskostnader hos tilbydere er alene forventet å gi vesentlige økte utgifter. Dersom det legges opp til en modell som innebærer å legge mer av kostnadsbyrden over på myndighetene, vil dette øke utgiftene ytterligere. I tillegg forutsetter forslaget tilpasninger i politiets IKT-systemer for å kunne motta, dekode og lagre data fra tilbydere. I høringsnotatet vises det til at tilpasninger i politiets system vil være en del av politiets løpende utviklingskostnader på området, og håndteres innen gjeldende budsjettrammer. Derav at ikrafttredelse av lovforslaget ikke i stor grad vil påvirke politiets behov for å gjøre justeringer i sine IKT-systemer.

Slike løsninger må først utvikles og deretter forvaltes på en god måte. Dette er ikke hensyntatt i dagens utviklingsportefølje i politiet. Kostnadene avhenger blant annet av valg av løsninger, typisk eventuelle selvbetjeningsløsninger eller lignende, og kan derfor vanskelig kostnadsettes nå. Mulige løsninger vil kreve ytterligere utredninger. Vi vil derfor påpeke at det også her vil påløpe kostnader ut over dagens utvikling- og driftskostnader. For øvrig må det påpekes at politiet generelt har et stort utviklingsbehov knyttet til modernisering og fornyelse av en rekke tjenesteområder og at utviklingstiltak må tilpasses etatens gjennomføringsevne.

Den økonomiske situasjonen i politiet er stadig mer presset som en følge av en rekke føringer og krav. Uten særskilt finansiering er det fare for at de foreslåtte endringene ikke vil få de tilsiktede virkninger, eventuelt at det vil påvirke måloppnåelse på øvrige prioriterte områder i politiet.

Oppsummert er det Politidirektoratets vurdering at de økonomiske og administrative konsekvenser for politiet må utredes nærmere i det videre arbeidet. Videre at de økonomiske og administrative konsekvensene ikke kan dekkes innenfor eksisterende budsjettrammer, men at iverksettelse forutsetter tilleggsbevilgninger til politiet over statsbudsjettet.

Med hilsen

Håkon Skulstad
assisterende politidirektør

Kristine Langkaas
seksjonssjef

Dokumentet er elektronisk godkjent uten signatur.

Vedlegg:
- Høringssvar fra Politihøgskolen av 7. desember 2020

- Høringssvar fra Sør-Øst politidistrikt av 14. januar 2021
- Høringssvar fra Innlandet politidistrikt av 18. januar 2021
- Høringssvar fra Sør-Vest politidistrikt av 18. januar 2021
- Høringssvar fra Nordland politidistrikt av 14. desember 2020
- Høringssvar fra Øst politidistrikt av 8. januar 2021
- Høringssvar fra Oslo politidistrikt av 14. januar 2021
- Høringssvar fra Trøndelag politidistrikt av 14. januar 2021
- Høringssvar fra Kripos av 15. januar 2021 med vedlegg
- Høringssvar fra Politiets utlendingsenhet av 18. januar 2021
- Høringssvar fra Økokrim av 11. januar 2021 (sendt departementet)

Kopi: Justis- og beredskapsdepartementet

POLITIHØGSKOLEN

Politidirektoratet
Postboks 2090 Vika
0125 OSLO

NORWEGIAN POLICE UNIVERSITY COLLEGE

Deres referanse:	Vår referanse:	Dato:
20/126210 - 6	20/02918-3	07.12.2020

HØRINGSSVAR - ENDRINGER I EKOMLOVEN (LAGRING AV IP-ADRESSER MV.)

Det vises til brev fra POD av 26.10.2020, høringsbrev fra KMD av 9.10.2020 og vedlagte høringsnotat.

Når det gjelder hva som skal lagres, så støtter Politihøgskolen departementets vurdering og mener forslaget til lovtekst dekker politiets behov.

Det foreslås en lagringstid på seks, ni eller tolv måneder, mens øvrige nordiske land opererer i spennet ni til tolv måneder. En lagringstid på ni til tolv måneder vil være fornuftig, både for å harmonisere praksis i de nordiske landene og for å avhjelpe politiets behov.

Det stilles et krav om at utlevering skal betinge at det dreier seg om alvorlig kriminalitet for at kravet til proporsjonalitet skal være oppfylt jf. Kommunikasjonsdirektivet. Det oppstilles ikke noen standard eller beskrivelse av «alvorlig kriminalitet». Det politiet anser som mindre alvorlig kan oppfattes som alvorlig av den som utsettes for handlingen.

Etter en drøfting av om hjemmel til innhenting skal baseres på at det mistenkes brudd på bestemte straffebud eller straffebud med en viss strafferamme, foreslår Departementet at lovteksten legger til grunn en generell strafferamme på ett til to års fengsel.

Innhenting av abonnementsinformasjon vil ikke være å anse som et tvangsmiddel, slik rettsreglene er foreslått innført. Det er likevel fornuftig å se hen til reglene om bruk av tvangsmidler, da opplysningene kan bli brukt som bevis i straffesaker, og det vil her, som ved bruk av tvangsmidler, være en proporsjonalitetsvurdering, selv om den her legges på generelt nivå i lovreguleringen, og ikke i det enkelte særskilte tilfelle. Til sammenligning kreves det, for å foreta en pågripelse, at siktede mistenkes for en handling som kan medføre fengsel i minst seks måneder, mens for å ransake kreves det at man etterforsker et forhold som kan medføre frihetsstraff. Det er urimelig at et slikt mindre inngrep skal kreve et forutgående straffbart forhold av større alvorlighet, selv om det ikke vil foretas en urimelighetsvurdering i den enkelte sak. Terskelen departementet legger til grunn synes høy i forhold til graden av inngrep.

Forslaget åpner også for at politiet skal kunne innhente abonnementsinformasjon på IP-adresser i saker utenfor straffesak, slik praksis er i dag. Det er i utgangspunktet vanskelig å se noen god grunn til at det skal stilles strengere krav enn i dagens regelverk, selv om lagringstiden utvides. Det er de samme opplysningene som utleveres, og det er den samme relativt svake inngripen i personvernet som skjer. På den annen side stiller både kommunikasjonsdirektivet og EMDs praksis krav om høyere terskel. Det bør likevel ikke stilles strengere krav til utlevering av abonnementsinformasjon enn å foreta en ransaking, som nok oppleves mer inngripende i privatlivet. En regel som oppstiller et krav om at det foreligger et straffbart forhold som kan innebære frihetsstraff bør således være dekkende, og det vil da sannsynligvis ikke være behov for en oppramsing av alternative straffebud som har lavere strafferamme. Dette da de fleste straffbare forhold som vil medføre behov for å innhente slike opplysninger vil ha strafferamme som inkluderer frihetsstraff.

Et spørsmål som fremstår som ubesvart er om det vil kreves at det oppgis ovenfor internettleverandøren hvilket straffbart forhold som etterforskes, eller som det vil påhvile påtalemyndigheten eller politiet å sørge for at man ikke ber om opplysninger der de formelle vilkårene ikke er oppfylt.

Det er positivt at departementet foreslår å beholde dagens løsning, med at opplysningene kan innhentes av politi og påtalemyndighet. En løsning med prøving av vilkårene for domstolene ville medført en unødig ekstrabelastning både for domstolene som skal behandle sakene og påtalemyndigheten som skal fremme sakene for domstolene. Den samme konklusjonen vil gjelde om NKOM skulle behandlet forespørslene.

Politihøgskolen er positive til lovforslag. Lengre lagringstid på abonnementsinformasjon på IP-adresser har vært savnet hos politiet lenge og endringen medfører en tilpasning til regelverk i de øvrige europeiske land. Det er snakk om relativt små inngrep i personvernet som støtter hensynet til effektiv etterforskning av straffbare forhold, som i stadig større grad foregår helt eller delvis over internett, eller der sentrale bevis forefinnes på internett.

Med hilsen

Nina Skarpenes
Rektor

Bodil Haug
Seniorrådgiver

Dokumentet er elektronisk godkjent uten signatur.

Saksbehandler:
Robert Furuhaug

POLITIET

Politidirektoratet
Postboks 2090 Vika
0125 Oslo

Sør-Øst politidistrikt

Deres referanse:	Vår referanse:	Dato:
20/126210-9	20/126210 - 30	14.01.2021

Høringssvar fra Sør-Øst politidistrikt – Endringer i ekomloven (lagring av IP-adresser mv.)

1. Innledning:

Det foreslås innføring av en plikt for tilbydere av ekomtjenester til å lagre IP-adresser, slik at politiet kan få tilgang til IP-adressene for å bekjempe alvorlig kriminalitet. Det bes særlig om høringsinstansenes syn på hvilket strafferammekrav som bør oppstilles, og på hvor lang lagringstiden bør være. Under følger Sør-Øst politidistrikts høringssvar.

2. Bør det innføres plikt til IP-lagring?

Sør-Øst politidistrikt mener lagring av IP-adresser er et svært viktig verktøy i kriminalbekjempelsen, og at slike opplysninger vil bidra til å ivareta den enkeltes vern mot kriminalitet som staten er forpliktet til via internasjonale avtaler. Det vises her blant annet til følgende uttalelse fra Departementet:

> "Departementene viser videre til at EMK artikkel 8 også innebærer en positiv forpliktelse til å muliggjøre etterforskning av lovbrudd, jf. K.U mot Finland nevnt i punkt 4.1 over, der EMK artikkel 8 ble ansett å ha blitt krenket fordi den finske lovgivningen ikke i tilstrekkelig grad åpnet for utlevering av IP-informasjon."

Lagringsplikten for IP-adresser utgjør et langt mindre inngrep enn lagring av teledata. Slik lagring vil ikke kunne vise hva abonnentene har foretatt seg på nettet. Informasjon om IP-adresser omtales gjerne som abonnementsopplysninger eller brukerdata. Denne typen informasjon har først og fremst betydning for å kunne koble opplysninger om kommunikasjon til en bestemt abonnent. Lagringen av slik informasjon ivaretar legitime formål og er forholdsmessig når det gjøres for å bekjempe kriminalitet av en viss alvorlighetsgrad.

3. Hvem skal lagre?

Sør-Øst politidistrikt mener alle tilbydere må ha en lagringsplikt så lenge de tilbyr tjenester hvor sluttbruker gis tilgang til internett. Lagringsplikten må gjelde uavhengig av teknologisk plattform.

4. Hva skal lagres?

Sør-Øst politidistrikt mener det er hensiktsmessig å velge en mellomløsning ved utformingen av bestemmelsen, der lagringsplikten begrenses til det som er nødvendig, samtidig som det presiseres hva abonnenten skal kunne identifiseres med utgangspunkt i.

5. Hvordan og hvor skal data lagres?

Sør-Øst politidistrikt mener det ikke er behov for å stille krav til hvor dataene lagres eller skal lagres i tilbyderens egne systemer/infrastruktur. Begrunnelsene som er gitt i høringsnotatet er dekkende for vårt syn.

6. Lagringstid

Flere forhold taler for at IP-adresser bør ha en lang lagringstid. For det første kan det gå lang tid mellom når det straffbare forholdet begås og når det avdekkes. Særlig vil dette gjelde ved unge fornærmede som kan vente med å gå til politiet eller andre å anmelde forholdet. Videre kan etterforskingen avdekke forhold som er lang tilbake i tid. Gjennomgang av elektroniske databeslag kan også være tidkrevende og gjøre at det tar tid å finne frem til en eller flere IP-adresser.

Inngrepets styrke taler også for en lang lagringstid. Særlig gjelder dette når det settes opp mot alvorligheten i mange lovbrudd hvor slik informasjon er helt nødvendig.

Etter dette bør lagringstiden settes til 12 måneder, slik som i Danmark.

7. Materielle vilkår for utlevering, herunder hvilke strafferammekrav som bør oppstilles

På bakgrunn av EU-domstolens praksis, jf. avgjørelsen La Quadrature du Net, kan lagring av IP-adresser for kriminalitetsbekjempende formål bare rettferdiggjøres dersom formålet er å bekjempe «alvorlig kriminalitet».

Selv om en strafferamme på bot eller fengsel inntil 1 år isolert sett ikke er "alvorlig kriminalitet", har mange straffebestemmelser en slik strafferamme og kan oppleves som svært alvorlige av de som rammes av dem. Det vises her blant annet til straffeloven § 298 om seksuelt krenkende atferd uten samtykke, § 305 om seksuelt krenkende atferd mv. overfor barn under 16 år og § 306 om avtale om møte for å begå seksuelt overgrep. Her må det være hjemmel til å innhente opplysninger om IP-adressen for å kunne oppklare sakene.

Den generelle strafferammen bør settes til bot eller fengsel i inntil 2 år i kombinasjon med spesifikke straffebud der IP-adressen er av særlig stor betydning.

Det bør åpnes for utlevering av opplysninger når det er nødvendig for etterforskingen av en straffbar handling og å forebygge disse.

8. Utlevering av informasjon med utgangspunkt i både IP-adresse og abonnent?

Sør-Øst politidistrikt mener det bør åpnes for utlevering av IP-informasjon med utgangspunkt i en gitt abonnent. Dette bør bero på de samme vilkårene som for utlevering med utgangspunkt i en IP-adresse. Begrunnelsene som er gitt i høringsnotatet er dekkende for vårt syn.

9. Prosessuelle garantier ved utlevering

Utlevering av abonnementsopplysninger til en IP-adresse bør besluttes av påtalemyndigheten. Det skal foretas en nødvendighetsvurdering og en vurdering av hvilket straffebud som handlingen rammes av. Dette tilligger påtalemyndigheten å vurdere. Det anses ikke nødvendig å forelegge spørsmålet for domstolen.

10. Bruk av opplysninger om IP-adresser i sivile saker

Sør-Øst politidistrikt har ingen innspill på bruk av opplysninger om IP-adresser i sivile saker.

Med hilsen

Per Thomas Omholt
Politiinspektør

Dokumentet er elektronisk godkjent uten signatur.

POLITIET

Politidirektoratet
Postboks 2090 Vika
0125 Oslo

Innlandet politidistrikt

Deres referanse:	Vår referanse:	Dato:
	20/126210 - 41	18.01.2021

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

Det vises til bev av 11. desember 2020 fra Politidirektoratet om forslag til endringer i lov om elektronisk kommunikasjon (ekomloven).

Sentralt i endringsforslaget er at det innføres en plikt for tilbydere av ekomtjenester til å lagre IP-adresser, slik at politiet kan få tilgang til IP-adressene for å forebygge eller etterforske alvorlig kriminalitet.

Departementene fremholder i høringsnotatet at endringsforslaget blant annet vil kunne bidra til å forhindre og oppklare nettkriminalitet, og være et viktig virkemiddel for å oppnå FNs bærekraftmål 16.2 om å stanse overgrep, utnytting, menneskehandel og alle former for vold mot og tortur av barn.

Endringsforslaget vil også være et viktig virkemiddel for å gjøre staten i stand til å oppfylle etterforskningsplikten gitt i EMD for å beskytte enkeltpersoner mot alvorlig kriminalitet, som for eksempel vold og seksuelle overgrep, begått av andre privatpersoner.

Utredningen fremstår som grundig og gjennomtenkt. Innlandet politidistrikt stiller seg svært positive til at det foreslås lovendringer, som ivaretar hensynet til samfunnets kriminalitetsbekjempelse.

Høringsinstansene bes særskilt tilkjennegi sitt syn på hvilket strafferammekrav som bør oppstilles, og hvor lang lagringstiden bør være.

Når det gjelder de konkrete forslagene i høringsnotatet/lovforslag (pkt. 8, s. 39-40 flg.) og de alternativene som oppstilles har vi følgende kommentarer:

§ 2-8 a Plikt til lagring av IP-adresser
Det er svært viktig at Litra b) kommer med i lovendringen, slik at politiet også får s.k. "portnummer" der flere har samme IP adresse. Dersom man ikke har denne muligheten vil man i mange tilfeller komme i en situasjon hvor vi står med en større mengde potensielle brukere uten mulighet til å identifisere den eller de konkrete brukerne det er grunnlag for å rette mistenke mot. Uten denne adgangen vil politiets mulighet til å avdekke, avverge, stanse og forfølge alvorlig kriminalitet bli vanskeliggjort. Det vil også i et rettssikkerhetsperspektiv kunne føre til urettmessige mistanker mot personer, om denne adgangen ikke gis.

I Danmark er lagringstiden 12 måneder, i Sverige 10 måneder og i Finland 9 måneder. Lagringslengden i Norge bør gjenspeile nivået i de andre nordiske landene, som det er naturlig å sammenligne oss med, ref. pkt. 7.4. Lagringstiden frarådes kun å bli 6 måneder. Pliktig lagringslengde bør være i 12 måneder, minimum 9 måneder. Hovedargumentet for dette er å gi politiet en reell mulighet til å bekjempe alvorlig kriminalitet. Av erfaring vet vi at det ved etterforsking av straffesaker er lett å komme tidsmessig på etterskudd i bevisinnhentingen. Både som en følge av sakenes karakter, når anmeldelse forelå, men også som en følge av kapasitet og restanseutfordringer.

Når det gjelder kostnadsberegning mener vi at modell E vil være best for politiet.

§ 2-8 b Utlevering av opplysninger lagret etter § 2-8 a
Det er viktig at det det blir gitt anledning til å innhente opplysninger i både forebyggende- og etterforskingsøyemed.

I praksis vil den foreslåtte lovendringen medføre en innskjerping i forhold til dagens rettstilstand, som i dag kan skje uten hensyn til strafferamme/bestemte straffebud. Det er dog godt akseptabelt sett hen til fordelene med lengre lagringstid. Men det må sikres at politiet kan innhente opplysninger i relevante saker.

Vi mener derfor at strafferammevilkåret ikke bør settes høyere enn et år. Som det fremkommer i høringsnotatets side *35:*

"Informasjon om IP-adresser kan være av stor betydning for etterforskningen av en rekke former for kriminalitet som isolert sett ikke nødvendigvis kan medføre lange fengselsstraffer."

Skulle strafferammevilkåret settes høyere, for eksempel til to år, må man i tilfelle sørge for at en del spesifikke lovbrudd/bestemmelser med lavere strafferamme også omfattes. Uten at disse inntas særskilt som hjemmelsgrunnlag, vil det medføre store utfordringer for etterforskning av sakene.

Det vises til riksadvokatens høringsbrev av 11. dm. Vi slutter oss til de synspunkter som fremkommer der.

Med hilsen

Johan Martin Welhaven
Politiinspektør
Leder for felles enhet for påtale

Dokumentet er elektronisk godkjent uten signatur.

POLITIET

Politidirektoratet
Postboks 2090 Vika
0125 Oslo

Sør-Vest politidistrikt

Deres referanse:	Vår referanse:	Dato:
	20/126210 - 39	18.01.2021

Høring - Endringer i ekomloven (lagring av IP-adresser mv.)

Innledning

Det vises til brev fra Politidirektoratet av 11. desember 2020 med utsatt frist for å komme med innspill til høringen innen 18. januar 2021. Sør-Vest politidistrikt støtter forslaget til departementene om at det skal innføres en plikt for tilbydere av ekomtjenester til å lagre IP-adresser – herunder lagring av informasjon om hvilke portnumre på abonnementssiden som er benyttet ved kommunikasjonen.

Høringsnotatet redegjør godt for de ulike hensyn som må vurderes i spørsmålet om hvorvidt det skal gis pålegg om lagring og innføres en plikt til å utlevere opplysninger til politiet. Lagringsplikten må omfatte alle opplysninger som er nødvendige for å nå formålet med lagringen. Sør-Vest politidistrikt vil knytte noen kommentarer til høringsnotatet.

Utfordringer

Kripos gikk 10. februar i fjor ut med at de i 2019 måtte forkaste hvert femte tips om nettovergrep på grunn av manglende lagringsplikt av IP-adresser. Hver og en av disse sakene kan være svært alvorlig for dem det gjelder og pågående seksuelle overgrep kunne vært stanset.

Sør-Vest politidistrikt har gjennom sitt etterforskningsprosjekt Operasjon Spiderweb, en rekke ganger av samme grunn endt opp med å unnlate å følge opp IP- adresser som har utgjort motpart i kommunikasjon med gjerningspersoner som prosjektet har hatt under etterforskning. Politidistriktet har også eksempel på at den gjeldende korte lagringstida på 21 dager bare så vidt har vært nok til å identifisere en gjerningsperson med svært høy operasjonssikkerhet som begikk voldtekter av barn over hele landet. Gjerningspersonen ville antakelig ikke blitt identifisert uten lagringen.

Dette viser at Datatilsynets fortolkning av personopplysningsloven, personvernhensyn og vurdering av lagringsbehovet for IP-adresse med slettefrist for IP- opplysninger senest etter 21 dager er i sterk motstrid med de behov politiet har for lagring av abonnementsinformasjon av IP-adresser.

Overgrepsmateriale er i praksis produkt av overgrep mot barn, hvor langt fra alle overgrepene er dokumentert ved bilder eller videoer. Sør-Vest politidistrikt mener at Norge ved å opprettholde Datatilsynets praksis ikke har fulgt opp sine internasjonale konvensjonsforpliktelser, verken i forhold til Europarådet eller FN når det gjelder overgrep mot barn.

Det er ikke bare hensynet til å avdekke gjerningspersoner som tilsier lagring av opplysninger om IP- adresser, men også hensynet til å identifisere fornærmede eller vitner. I nettovergrepssaker er det kun unntaksvis at gjerningspersoner benytter egne navn eller korrekt personalia i sin kontakt med ofre eller likesinnede. Mange barn og unge benytter også uriktig personalia på internettbaserte kommunikasjonsplattformer og IP- lagring vil derfor i mange tilfeller være avgjørende for å få identifisert både gjerningsperson, fornærmede og vitner.

Strafferammekrav

Flere av de omfattende nettovergrepssakene, også i vårt politidistrikt, har startet med utgangspunkt i mistanke om overtredelse av straffeloven § 305 – seksuelt krenkende atferd overfor barn under 16 år. Alvorlighetsgraden har først i ettertid blitt avklart ved hjelp av avhør og beslag. Selv om strafferammen for § 305 fra 01.01.21 har økt fra 1 til 2 år så er det viktig at et strafferammekrav for utlevering av informasjon om IP-adresse ikke settes for høyt.

Strafferammen for overtredelse av straffeloven § 306 – avtale om møte for å begå seksuelt overgrep – er 1 år og avtale gjøres ofte over internett hvor identifisering av gjerningsperson gjennom IP-sporing i mange tilfeller er avgjørende. Strafferammekravet for utlevering av IP- informasjon bør derfor ikke settes høyere enn 1 år, men gjerne i kombinasjon med unntak for spesifikke straffebud hvor IP- informasjon er av særlig betydning.

Den svenske lovgivningen tar også hensyn til behovet for å sikre at opplysningene er tilgjengelig for å etterforske hendelser der personer er forsvunnet eller der det er fare for liv og helse. Deres lagringsplikt er ikke begrenset til etterforskning av "alvorlige straffbare" forhold og synes således ikke i harmoni med EU-domstolens dom av 6. oktober 2020 som høringsnotatet refererer til. Det er ikke fastslått i praksis hva som menes med alvorlig kriminalitet. Det bør i tråd med den svenske lovgivningen vurderes hvorvidt IP- informasjon kan utleveres til politiet ved behov i forbindelse med etterforskning av saker der personer er savnet under slike omstendigheter at det kan være fare for personens liv eller helse samt ved dødsfall og ulykker med personskade. Det er her verdt å nevne at mistenkelige dødsfall ikke rent sjelden ender opp i en drapsetterforskning og at informasjon om IP- adresser kan være avgjørende for å nå dit.

Lagringstid

Sør-Vest politidistrikt mener at hensynet til muligheten for å etterforske og oppklare alvorlig kriminalitet tilsier at lagringsperioden er lengst mulig, altså 1 år fra avslutning av kommunikasjonen. Det vil være en lagringstid som harmoniserer med de fleste land i Europa, inkludert de øvrige nordiske landene. I saker hvor IP- informasjon vil ha betydning som bevis har etterforskningen ofte pågått en stund. Nettovergrepssaker krever omfattende ressurser og er tidkrevende. Sør-Vest politidistrikt har i flere tilfeller opplevd å motta opptil 1 år gamle IP- adresser fra de store tjenestetilbyderne med base i USA. Siden IP- informasjon har vært avgjørende for å

komme videre etterforskningen så har disse sakene blitt lagt bort i mangel på informasjon som kan bidra til å identifisere gjerningspersoner.

Generelle betraktninger

Lagring av IP-adresse omfatter ikke lagring av informasjon om innholdet i abonnentens internettkommunikasjon, hvem abonnenten har vært i kontakt med, eller hvor abonnenten befinner seg. I seg selv vil informasjon om IP-adresser som hovedregel kun gi opplysning om at abonnenten har hatt internettilgang på et gitt tidspunkt. Det å avverge, redusere og oppklare alvorlig kriminalitet er ikke politiets ansvar alene. I en rettsstat må alle borgere, institusjoner og organer bidra siden bekjempelse av alvorlig kriminalitet er en forutsetning for at en rettsstat skal fungere. Dette bør også innebære tilbydere av ekomtjenester.

Selv om anonymiserings- og krypteringsløsninger benyttes vil lagring av IP- informasjon ha verdi som etterforskningsverktøy. Sør-Vest politidistrikt erfarer at kun et fåtall av gjerningspersonene har benyttet slike løsninger. Dersom dataene slettes må man spørre seg om det er meningsfull ressursbruk å prioritere arbeidet mot overgrepsbilder på nettet. Det har lite for seg å kriminalisere om man aktivt plikter å slette opplysninger som er sentrale for straffeforfølgningen.

Lagringsplikten må videre omfatte alle opplysninger som er nødvendige for å nå formålet med lagringen. Lovteksten og eventuelt forarbeidene må i størst mulig grad presisere at internettilbydere må forholde seg til lagringskravene og tilpasse sin teknologi og valg av systemer ut i fra dette. Hvis de av teknologiske årsaker legger inn en begrensning i sine plikter etter loven og dette ikke følges opp så vil regelverket fort kunne miste sin tiltenkte virkning.

Retten til privatliv etter EMK artikkel 8 omfatter også den fysiske og psykiske integritet og retten til å være i fred for kriminalitetsofre, noe som også taler for lagring av opplysninger om IP-adresser av hensyn til fornærmede. Staten har et ansvar for vern av borgerne. Inngrepet er nødvendig i et demokratisk samfunn, vil ha hjemmel i lov, har et legitimt formål og være forholdsmessig.

Med hilsen

Kristin Nord-Varhaug
Politiinspektør

Dokumentet er elektronisk godkjent uten signatur.

POLITIET

Politidirektoratet
Postboks 2090 Vika
0125 Oslo

Nordland politidistrikt

Deres referanse:	Vår referanse:	Dato:
	20/126210 - 25	14.12.2020

Høring - endringer i ekomloven (lagring av IP-adresser mv.) Svar fra Nordland politidistrikt

Nordland politidistrikt støtter en endring av regulering av lagring av IP-adresser og utlevering av disse i gitte tilfelle.

Dagens regulering oppfattes å være mangelfull ved at lagringstiden er svært kort, og praktiseres noe ulikt hos de ulike tilbydere.

Nordland politidistrikt har det siste året jobbet aktivt opp mot å avdekke overgrep begått på nett i distriktet. Gjennom dette har en dessverre brakt til erfaring at mange saker lar seg opplyse på en lite tilfredstillende måte ved at internettrafikk ikke lar seg spore tilbake ettersom IP-adresser og tilknyttet abonnement ikke har vært lagret. Slike saker er ofte tidkrevende, og avdekkes over tid, slik at i dagens regulering er sporene ofte slettet før man får hånd om disse.

En har også gjort seg erfaringer knyttet til andre typer kriminalitet enn overgrepssaker, særlig innenfor økonomisk kriminalitet på nettet, hvor spor er slettet når man kommer i posisjon til å etterspørre abonnementsopplysninger knyttet til en IP-adresse. Det er all grunn til å tro at denne kriminalitetstypen vil fortsette og øke i framtiden. I slike saker er det erfaringsmessig behov for å få rettslige kjennelser fra utlandet for å avdekke IP-adresse fra utenlandske tilbydere.

IP-adresser og abonnmentsopplysninger bør derfor lagres et år – 12 måneder.

De data som lagres bør være av en slik karakter at det er mulig å knytte abonnement til IP-adressen. Dette er særlig relevant for delte IP-adresser, hvor opplysninger som kan skille de ulike abonnentene fra hverandre må lagres i tilfelle senere utlevering.

En erkjenner at lagring av IP-adresser og abonnementsopplysninger har en sterk slagside mot retten til å være anonym og personvernet generelt. Det må derfor være klare skranker mot når politiet kan be om utlevering av slike opplysninger.

En er enig i at legalitetskontrollen er ivaretatt ved at utlevering kan besluttes av påtalemyndigheten i politiet. Påtalemyndigheten i politiet har primærkompetanse i svært mange av tvangsmidlene og er således vel vant med å forta de avveininger som må gjøres i slike saker. Tvangsmidlet anses ikke like inngripende som f.eks. en husransaking eller kommunikasjonskontroll og kompetansen bør derfor ikke legges til retten.

Det bør være en viss alvorlighet knyttet til de forhold hvor utlevering av IP-opplysninger besluttes. Herfra foreslås at forholdet må ha en strafferamme på minst tre år eller omfattes av straffeloven kapittel 26 før slike opplysninger kan besluttes utlevert. En unngår derved at de mindre forhold berettiger en slik utlevering. Samtidig omfattes deling av seksualiserte bilder, unønsket seksualiserte framstøt (strl. §§298/305), grooming §306 og andre mindre seksuallovbrudd som ofte skjer over nett.

Med hilsen

Stig Morten Løkkebakken
Politiinspektør

Dokumentet er elektronisk godkjent uten signatur.

POLITIET

Politidirektoratet
politidirektoratet@politiet.no

ØST POLITIDISTRIKT

Deres referanse:	Vår referanse:	Sted, Dato
20/126210-9		8.1.2021

HØRING– ENDRING I EKOMLOVEN (LAGRING AV IP-ADRESSER MV.)

Øst politidistrikt viser til politidirektoratets brev av 11. desember 2020 der Justis- og beredskapsdepartementet og Kommunal- og moderniseringsdepartementets høringsnotat om endringer i Ekomloven sendes politidistriktene for innspill. Svarfristen til Politidirektoratet er 18. januar 2021.

Øst politidistrikt har gjennomgått høringsnotatet og er i det vesentligste enige i de vurderinger som fremkommer i høringsnotatet og det samlede lovforslag. Endring i kriminalitetsbildet og kommunikasjon nødvendiggjør endring i gjeldende regelverk. Høringsnotatet er etter vårt syn grundig og gir et balansert bilde av behovet for en endring.

1. Behov for endringer i ekomloven

Øst politidistrikt har ved flere anledninger erfart at lagringstiden for IP-adresser er for kort med den følge at straffesaker må henlegges fordi gjerningspersonen ikke blir identifisert. Sporet etter lovbryteren slettes etter 21 dager. Internett og sosiale medier har gitt personer som vil begå, produsere og dele nettovergrep store muligheter. Den teknologiske utviklingen gjenspeiles i kriminalitetsbildet. Overgrep mot barn på nett er et økende problem. Det kommuniseres på ulike sosiale plattformer. Politidistriktet har erfart at det ofte kan ta opptil tre måneder før et selskap utleverer IP-adressen bak et brukernavn knyttet til et sosialt medium, eksempelvis "Snapchat". Ofte kan det også ta lang tid fra et straffbart forhold begås til det anmeldes.

En lengre lagring av IP-adresse vil være et viktig virkemiddel for politiet for å oppklare alvorlig kriminalitet. En lengre lagring vil ikke krenke personvernet eller ytringsfriheten etter vårt syn, det er ikke innholdsdata som etterspørres eller lagres,

men hvem som er oppført med aktuelt abonnement hos teletilbyder. Det er et stort behov for endring i ekomloven, en endring har vært etterlyst i flere år.

2. Utlevering av opplysninger til etterforskning, men også for å forebygge handling

Øst politidistrikt stiller seg bak forslaget om at opplysninger skal kunne utleveres i forbindelse med etterforskning av konkret sak og når det er nødvendig for å forebygge en straffbar handling. Informasjon om tilknytning mellom abonnent og IP-dresse er informasjon som kan være viktig for avverging og forebygging av lovbrudd. EMK artikkel 8 nr 2 innebærer en positiv forpliktelse til å muliggjøre etterforskning av lovbrudd.

3. Hvor lang bør lagringstiden være?

Formålet med endringen er å gi politiet et effektivt verktøy i kampen mot alvorlig kriminalitet i et digitalisert samfunn, og vil dermed komme samfunnet som helhet til gode. Politiets behov for opplysningene må avveies opp mot hensynet til kommunikasjonsvernet.

Øst politidistrikt fremhever at om lagring skal ha tilstrekkelig nytteverdi i kriminalitetsbekjempelsen, er det viktig at den ikke er for kort. Øst politidistrikt erfarer at det ofte er en tidkrevende prosess å hente ut IP-adresser fra utenlandske nettsteder/ sosiale medier. Ikke sjeldent avdekker man flere fornærmede eller siktede, det er omfattende beslag i saken, i tillegg til at det erfaringsmessig kan ta lang tid fra et straffbart forhold begås til det oppdages/anmeldes.

Ingen av våre nordiske naboland, som det er naturlig å sammenligne seg med, har en lagringstid på under ni måneder. I Sverige lagres opplysningene i ti måneder, Danmark tolv måneder og i Finland ni måneder.

Øst politidistrikt er av den oppfatning at en lagringstid med en kortere varighet enn ni måneder må unngås om formålet med endringen skal oppnås. En lagring på tolv måneder vil i størst grad ivareta politiets behov, ha et legitimt formål, og fremstå forholdsmessig. Effekten av en lagringstid på et år gir en større mulighet til å komme til bunns i hvem som kan være den skyldige, som igjen er til gunst for allmennheten.

4. Hvilket strafferammekrav bør oppstilles?

Øst politidistrikt stiller seg bak forslaget om at kriminaliteten må være av en viss alvorlighetsgrad slik at reglene om utlevering knyttes opp mot et generelt strafferammekrav, eventuelt i kombinasjon med nærmere bestemte straffebud der IP-informasjon er av særlig stor betydning.

.

Øst-politidistrikt har i flere saker erfart at mindre alvorlige straffbare handlinger med lav strafferamme fungerer som inngang til pågripelse/ransaking, eksempelvis overtredelse av straffeloven § 305, seksuelt krenkende atferd overfor barn under seksten år, som har en strafferamme på fengsel inntil 1 år. Eksempelvis gjelder dette et barn som får tilsendt et bilde av kjønnsorgan. I forbindelse med etterforskning og gjennomgang av konkret beslag har politiet senere avdekket grovere straffbare handlinger mot flere fornærmede. Om man ikke gis mulighet til å innhente IP-adresse ved mindre alvorlige seksuelle overgrep på internett, risikerer man at man går glipp av å avdekke grovere straffbare handlinger /seksuelle overgrep.

Stadig mer av kommunikasjonen i samfunnet skjer via internnettbaserte løsninger. Opplysninger om nettbasert kommunikasjon blir dermed stadig viktigere i alle typer saker. Informasjon om en IP-adresse vil kunne være av stor betydning for etterforskning av en rekke former for kriminalitet som ikke nødvendigvis gir lange fengselsstraffer. Handlingene kan oppleves som alvorlig for de som rammes.

Øst-politidistrikt mener derfor at det er hensiktsmessig å fastsette strafferammekravet til fengsel i 1år. En vil med dette gis en større mulighet til å avdekke kriminalitet.

Om strafferammekravet settes til to års fengsel, fremstår det som formålstjenlig å angi nærmere bestemte straffebud hvor IP-informasjon er særlig viktig, som "*etter loven kan medføre straff av fengsel i 2 år eller mer, eller som rammes av straffelovens kapittel 26 om seksuallovbrudd.*

Med hilsen

Mona Elin Hertzenberg
påtaleleder

Saksbehandler:
Politiadvokat Anette Sogn

Dokumentet er godkjent elektronisk

POLITIET

Politidirektoratet
Postmottak POD via Websak

Oslo politidistrikt

Deres referanse:	Vår referanse:	Dato:
	20/126210 - 32	14.01.2021

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

Det vises til Kommunal- og moderniseringsdepartementet og Justis- og beredskapsdepartementets høringsbrev av 9. oktober 2020 med tilhørende høringsnotat, med forslag om å innføre en plikt for tilbydere av ekom-tjenester til å lagre IP-adresser til bruk i kriminalitetsbekjempelsen. Høringsfristen ble satt til 11. januar 2021, og senere forlenget til 24.januar 2021. Frist for innspill til Politidirektoratet ble satt til 18. januar 2021.

1. Innledning

Lagring av IP-adresser vil være et viktig bidrag for å styrke og effektivisere politiets internettrelaterte etterforsking. Hele samfunnet stadig mer digitalisert og Oslo politidistrikt ser at også kriminaliteten i stadig større grad flytter seg over i det digitale rom. Det er flere områder hvor denne utviklingen er særlig tydelig, blant annet nettovergrep mot barn, økonomisk kriminalitet, grov narkotikakriminalitet og organisert kriminalitet. Oslo politidistrikt har spesialiserte etterforskningsmiljøer innenfor disse kriminalitetsområdene.

I saker der det benyttes skjulte metoder som kommunikasjonskontroll og IP-basert kommunikasjonskontroll (data fra internett trafikk) har en ikke nødvendigvis en fullstendig forståelse av viktigheten knyttet til en kommunikasjon, på tidspunktet når selve kommunikasjonen foregår. Det vil gjerne fremkomme på et senere tidspunkt når en ser bevisbildet under ett, noe som ofte tar lang tid i større og alvorlige sakskomplekser. I lys av dette er det viktig i slike saker å ha mulighet til å innhente relevant informasjon knyttet til bl.a. lagring av IP-adresser i et tidsrom utover det som dagens regelverk gir muligheter for.

2. Balansering av hensyn

Det er ofte krevende å finne en god og riktig balanse mellom kriminalitetsbekjempelse på den ene siden og behovet for kommunikasjonsvern og personvern på den andre siden. Informasjon om

hvilke IP-adresser ulike abonnenter er tildelt vil ikke i seg selv gi informasjon om hvem abonnenten har kommunisert med, innholdet i kommunikasjonen eller hvor vedkommende befant seg. En plikt til lagring av IP-adresser som gir abonnentsopplysninger/brukerdata, vil således være mindre inngripende for kommunikasjonsvernet enn en lagringsplikt for historiske trafikkdata fra tjenestetilbydere.

Etter Oslo politidistrikt sin oppfatning, vil lagring av IP-adresser som foreslått med begrensninger i form av materielle vilkår for utlevering utgjøre et beskjedent inngrep ovenfor den enkelte kontra det som kan oppnås. Avveining av de ulike hensyn her, tilsier at ansvaret for vern av enkeltindividet og samfunnet mot kriminalitet bør gå foran kommunikasjonsvernet. Lagring av IP-adresser og utlevering av informasjon i konkrete straffesaker anses viktig ikke bare for å avdekke en gjerningsperson, men også for å utelukke en person fra mistanke og ikke minst identifisere ofre for alvorlige straffbare handlinger.

Selv om kriminelle i dag i økende grad benytter krypterings- og anonymiseringsløsninger, ser en at lagring av IP-adresser vil kunne få betydning i en rekke saker.

3. Korte betraktninger om VPN-tjenester

Bruken av VPN-tjenester er omtalt i høringsnotatet. VPN-tjenester utgjør en av fremtidens klart største tekniske utfordringer ved bekjempelse av internettrelaterte overgrep mot barn. VPN-tjenester med hovedsete og/eller serverparker i Norge er i dag ikke lovregulert. Om det ikke er tema i denne omgang, mener OPD at man må se nærmere på lovregulering av VPN-tjenester i Norge. Hertil bemerkes at dette er en problemstilling som naturligvis går på tvers av landegrenser, og at det er behov for internasjonalt samarbeid og regulering med norsk deltakelse.

Kommentar til enkeltpunkter i forslaget. Til pkt. 7.2 – særskilte problemstillinger knyttet til deling av IP-adresser mellom abonnenter

Oslo politidistrikt er enig i forslaget om lagring av portinformasjon. Manglende lagring av portinformasjon har hittil gjort det vanskeligere å identifisere gjerningspersoner under etterforsking av straffesaker. Manglende lagring av portinformasjon vil kunne føre til en lovregulering som slår tilfeldig ut i overgangsfasen frem til IPv6 er ferdig integrert. Overgangsperioden mellom IPv4 og IPv6 vil slik en forstår det kunne ta mange år. En løsning hvor muligheten til å identifisere disponenten beror på tilbyderens tekniske løsning synes å være i dårlig overensstemmelse med likhetsprinsippet, og vil potensielt gi lovendringen mindre effekt.

Ulik mulighet til å identifisere brukere av IPv4 og IPv6 kan også medføre at datakyndige brukere som ønsker å forhindre identifisering bevisst velger å bruke IPv4 med portinformasjon.

3.1. Til pkt. 7.4 Lagringstid

Oslo politidistrikt mener at en lagringstid på minst tolv måneder er påkrevet dersom formålet med lagring av IP-adresser skal oppnås. Fordelene knyttet til forslaget synes langt flere enn betenkelighetene, og lagringen i seg selv anses heller ikke som særlig inngripende. Utleveringen vil uansett begrenses til forebygging og etterforsking av alvorlige saker, jf. under om strafferammekrav og nødvendighetskrav.

Ofte kommer anmeldelsen av et straffbart forhold inn i ettertid, og det gjelder ikke minst i seksuallovbruddsakene. Det kan videre ta tid før et straffbart forhold avdekkes eller etterforskningen av saken kan være tidkrevende. Som eksempel på sistnevnte nevnes utfordringer knyttet til saker med store beslag og tilgang til enkelte beslag hvor gjerningspersonen har forsøkt å vanskeliggjøre tilgangen/skjule spor. Anslaget i høringsnotatet på 3-4 uker for å få svar på anmodninger fra utenlandske tjenestetilbydere synes å være optimistisk utfra våre erfaringer.

Dersom man skulle kommet til at lagring i 12 måneder er for lenge, bør mellomløsninger vurderes som sikrer tilstrekkelig lang lagring i de alvorligste sakene. En mulighet kan være å lagre IP-informasjon i 12 måneder, men heve strafferammekravet til mer enn 1 år for utlevering i perioden 6-12 måneder. I særlig alvorlige saker, og hertil alle saker som gjelder seksuallovbrudd mot barn inntatt i straffeloven kap. 26 om seksuallovbrudd, bør IP-informasjon kunne utleveres inntil 12 måneder.

3.2. Til pkt. 7.5 Materielle vilkår for utlevering

Oslo politidistrikt er enig i at det bør settes klare og entydige vilkår for utlevering av abonnementsinformasjon, herunder både med utgangspunkt i IP-adresser og med utgangspunkt i abonnentens navn eller andre identifiserende opplysninger.

Strafferammekravet bør settes til ett år. Dette vil sikre at det kan innhentes abonnementsinformasjon i tilknytning til IP-adresser i saker som gjelder seksuallovbrudd mot barn etter straffelovens bestemmelser, samt de sentrale økonomiske straffelovbrudd. For oppfylle formålet med en innføring, er det avgjørende at også overtredelser av strl. § 305 og strl. § 306 inkluderes. Begge lovbud har en strafferamme på ett år.

Vi erfarer en stadig økning i internettrelaterte seksuallovbrudd mot barn, og vurderer tilgangen på abonnementsinformasjon tilknyttet IP-adresser som en helt sentral og viktig suksessfaktor i

bekjempelsen av internettrelaterte overgrep mot barn. I saker som gjelder nettovergrep mot mindreårige kan for eksempel ulike straffebud være overtrådt overfor ulike fornærmede, og det fremstår som urimelig at ikke å kunne innhente denne type informasjon der man for eksempel står ovenfor en 12-åring fornærmet som er tvunget eller forledet av en voksen til å sende seksualiserte bilder av seg selv over internett (strl. § 305 bokstav b).

Selv om det nok er ved etterforskning at forslaget har sin største relevans, er Oslo politidistrikt enig i at det samtidig bør lovreguleres en adgang til å utlevere opplysninger for å forebygge handlinger av tilsvarende alvorlighet.

Kravet om nødvendighet for at utlevering skal finne sted vil sikre at det kun er opplysninger av en viss betydning i den konkrete saken som utleveres.

3.3. Til pkt 7.5.2 Utlevering av informasjon med utgangspunkt i både IP-adresse og abonnent?

Oslo politidistrikt støtter forslaget om at det også skal være adgang til å kreve utlevert informasjon med utgangspunkt i abonnent, ikke bare med utgangspunkt i IP-adresse. Departementets begrunnelse tiltres.

Denne plikten fremgår imidlertid ikke entydig av ordlyden i endringsforslaget. Lovteksten i det endelige forslaget bør spesifisere at plikten også omfatter plikt til å utlevere informasjon med utgangspunkt i abonnement. Alternativt må dette tydeliggjøres i forskrift, jf. utkastets tredje ledd.

3.4. Tidsfrist for utlevering av informasjon

Oslo politidistrikt anbefaler at lovforslaget eller forskriften bør stille konkrete krav til responstid knyttet til utlevering av IP-informasjon. Vi erfarer i dag at det er store forskjeller mellom de ulike tilbyderne i forhold til responstid på politiets anmodninger.

3.5. Til pkt. 10 Kostnadsfordelingsmodell

Oslo politidistrikt er enig med departementet i at finansieringsmodellen må være slik at tilbyderne har et incitament til å lage et kostnadseffektivt system. Dette innebærer at man må unngå et system der tilbyderne tjener penger på å gi politiet informasjon.

Med utgangspunkt i tilbydernes plikt til å tilrettelegge nett og tjeneste for å sikre lovbestemt tilgang til informasjon etter ekomloven § 2-8, er det departementets modell C som ligger tettest

opp til dagens praktisering av kostnadsfordelingen mellom politi og tilbydere. Dersom det velges en annen modell enn den som har vært praktisert hittil bør det begrunnes særskilt.

Med hilsen

Beate Gangås
politimester

POLITIET

Politidirektoratet
Postboks 2090 Vika
0125 Oslo

Trøndelag politidistrikt

Deres referanse:	Vår referanse:	Dato:
	20/126210 - 34	14.01.2021

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

Det vises til høringsbrev av 9. oktober 2020 fra Kommunal- og moderniseringsdepartementet og Justis- og beredskapsdepartementet om forslag til endringer i lov 4. juli 2003 nr. 83 om elektronisk kommunikasjon (ekomloven), samt brev av 11. desember 2020 fra Politidirektoratet.

Når det gjelder pkt. 7.4 så støttes forslaget om en lagringstid for opplysninger om IP-adresser mm. på 12 måneder. Et slikt tiltak vil være lite inngripende da opplysningene som lagres ikke er av sensitiv art. Dette er vurdert opp mot behovet for slik lagringstid når det gjelder kriminalitetsbekjempelsen.

Lengre lagringstid vil også øke rettsikkerheten og treffsikkerheten ved IP-sporing når man slipper å involvere og sammenligne IP-adresser eldre enn 3 uker med IP-logger innhentet av tredjeparts tilbyder, slik det gjøres i dag fra for eksempel Altinn, Schibsted osv.

Forslaget om at lagringsplikten knyttes til lovbrudd med en strafferamme på minst ett år støttes. Et høyere strafferammekrav vil gjøre at en del lovbrudd faller utenfor, noe som i så fall bør "repareres" ved en positiv oppregning av disse lovbruddene.

Men dersom lagringsplikten og politiets mulighet til å hente ut slik informasjon knyttes til forebygging eller etterforskning av straffbare forhold som nevnt vil dette begrense muligheten til å bruke opplysningene i etterretningsøyemed. Dette kan f.eks. dreie seg om å finne ut hvem som sender anonyme tips, evnt kontrollere at tipseren er den han utgir seg for, kartlegge miljøer på sosiale medier og undersøke hvem som befinner seg bak fiktive identiteter på nett.

Med hilsen

Nils Kristian Moe
Politimester

Jostein Dahlø
Pob.Saksbehandler

Dokumentet er elektronisk godkjent uten signatur.

POLITIET
KRIPOS

Politidirektoratet

NCIS NORWAY

Sendes i Websak til postmottak POD

Deres referanse:	Vår referanse:	Sted, Dato
20/126210	20/126366	Oslo, 15.1.2021

HØRING - ENDRING I EKOMLOVEN (LAGRING AV IP-ADRESSER MV)

Innføring av lagringsplikt for informasjon som kan bidra til identifisering av sluttbruker på internett vil gjøre politiet i stand til å forebygge, avverge og oppklare mer av den alvorlige kriminaliteten. Samfunnet blir i stadig større grad digitalisert og innenfor de fleste kriminalitetsområder er de involvertes bruk av dataverktøy viktige kilder til bevis. En lagringsplikt vil derfor være av stor betydning, ikke bare for innsatsen mot den såkalte "nettrelaterte" kriminaliteten, men for bekjempelsen av all form for kriminalitet hvor kommunikasjon eller annen aktivitet foregår på eller ved hjelp av internett.

Når det med begrunnelse i kriminalitetsbekjempelsen innføres pålegg om lagring av informasjon som politiet senere kan få bruk for, er det viktig å finne en god balanse mellom hensynet til kriminalitetsbekjempelse og hensynene til kommunikasjons- og personvern. Kripos mener at det i høringsnotatet langt på vei er gjort gode vurderinger i denne avveiningen.

Kripos har i lang tid påpekt at manglende tilgang til informasjon som knytter IP-adresser til abonnent er en stor utfordring i etterforskning og forebygging av stadig flere straffesaker. Vi har helt fra prosessen rundt Datalagringsdirektivet (DLD) for over ti år siden bidratt til gjentatte initiativ for å få en lagringsplikt på plass. I vårt høringssvar til direktivet ble lagringsbehovet utførlig beskrevet – også hva gjelder knytningen mellom IP-adresse og bruker. Behovet er i ettertid understreket i flere andre høringsprosesser, herunder blant annet i våre høringssvar knyttet til tiltak 14 og 15 i Justisdepartementets strategi for bekjempelse av IKT-kriminalitet. Alle tre høringssvar vedlegges.

Den teknologiske utviklingen etter DLD har økt behovet for data som kan identifisere sluttbrukere på internett og det finnes i dag knapt straffesakstyper hvor IP-adresser ikke kan ha betydning. I flere og flere etterforskninger blir det med hjemmel i straffeprosessloven tatt i beslag og begjært utlevert store menger data hvor bruk av tjenester på internett inngår. Dette kan for eksempel være IP-logger fra banker i store bedragerisaker eller brukerdata fra kommunikasjonstjenester på internett (e-post, Facebook, Instagram, WhatsApp osv.) i saker som omhandler narkotika, hvitvasking, bortføring, trusler, overgrep mot barn mv.

Kripos

Den nasjonale enhet for bekjempelse av organisert og annen alvorlig kriminalitet
Post: Postboks 2094 Vika, 0125 Oslo
Besøk:

Tlf: 23 20 80 00
Faks: 23 20 88 80
E-post: kripos@politiet.no

Org. nr.: 974 760 827
Giro: 7694.05.17962
www.politi.no

Identifikatoren i slike data er ofte en IP-adresse, det vil si at politiet ut fra dataene alene ikke kan identifisere hvilke personer som for eksempel har sendt trusselen, tatt opp lånet med falsk identitet eller delt/lastet ned overgrepsmaterialet, men bare ser hvilke IP-adresser vedkommende har benyttet. For å identifisere gjerningspersonen i disse tilfellene må dataene som politiet har i etterforskningsmaterialet berikes med informasjon om hvem som har benyttet IP-adressen på det aktuelle tidspunktet.

Gjennom skjulte etterforskningsmetoder som kommunikasjonskontroll og dataavlesing fanger politiet også data hvor man kun har en IP-adresse som identifikator. Også her er politiet avhengig av abonnementsinformasjon for å komme videre i saken, typisk for identifikasjon av gjerningsmann, fornærmet eller vitner.

Logging av IP-adresser inngår videre som en del av sikkerhetsmekanismene til tjenestetilbydere på internett som nettbanker, Altinn, Skatteetaten, mv og ved bruk av sikre digitale ID-er som BankID. Selve IP-loggene lagres i lang tid, mens koblingen mellom abonnent og IP-adresse i dag lagres i inntil 21 dager dersom den lagres i det hele tatt. Disse sikkerhetsmekanismene har en redusert funksjon om man i etterkant, ved lovbrudd eller andre uregelmessigheter, ikke kan finne ut hvem som var involvert i den aktuelle datatrafikken fordi data som knytter IP adresse til bruker ikke er lagret.

Det foregående viser at behovet for den lagring som nå foreslås har økt vesentlig i tiden etter DLD-prosessen. I stadig flere etterforskninger får politiet kjennskap til IP-adresser som kunne løse saken dersom disse dataene kunne berikes med abonnementsinformasjon. Svært ofte er dette imidlertid ikke mulig, da dataene som kunne identifisert brukerne er slettet eller ikke lagret i det hele tatt.

De følgende kommentarer knytter seg til høringsnotatets kapittel 7, 10 og 11.

KAPITTEL 7

7.3 Utforming av lagringsplikten

Det foreslås i høringsnotatet at alle tilbydere av internettilgang for allmennheten skal pålegges en lagringsplikt. Kripos gjorde i forbindelse med implementering av DLD oppmerksom på at det finnes flere store tilbydere av private nett som kommuner, skoler, hoteller, flyplasser og lignende hvor formålet med lagringsplikten ikke vil oppfylles. Det vises her til kapittel 3 i Kripos' høringsuttalelse av 10. april 2012 til den foreslåtte datalagringsforskriften. Uttalelsen ligger vedlagt.

Slik Kripos' forstår det nåværende forslaget til lagringsplikt vil det heller ikke denne gangen innføres en lagringsplikt for disse aktørene, noe som vi fremdeles mener er uheldig. Sett hen til hensynet til kriminalitetsbekjempelsen bør det foreligge en tilsvarende plikt for slike aktører til å lagre tildeling av interne IP-adresser og tidsrom, kombinert med en autentiseringsløsning for pålogging.

7.3.2 Hva skal lagres

Departementet foreslår lagring av "*de opplysninger som er nødvendige for å identifisere abonnenten med utgangspunkt i*":

a) *En IP-adresse og et tidspunkt for kommunikasjon, eller*
b) *En offentlig IP-adresse, et tidspunkt for kommunikasjon og portnummer benyttet for kommunikasjonen, dersom samme offentlige IP-adresse tildeles flere abonnenter samtidig.*

Kripos er enig i at lagringsplikten må omfatte data som gjør at identifisering er mulig også hvor NAT-teknologi benyttes. Til tross for utfordringene for tilbyderne med å vite hvilke typer data de skal lagre, foretrekker Kripos likevel at lagringsplikten knyttes opp mot et teknologinøytralt begrep i retning av *«de opplysninger som er nødvendige for å identifisere abonnenten»*. En nærmere presisering av hvilke typer data som til enhver tid skal lagres, kan om nødvendig bestemmes i forskrift. Det sentrale er uansett om de opplysningene som lagres faktisk kan identifisere abonnenten til internettaksessen slik at det er mulig for politiet å identifisere sluttbruker.

Kripos er ikke kjent med om det i dag benyttes teknologi hvor det ville være nødvendig å lagre eksempelvis IP-adresse og portnummer på destinasjonssiden for å kunne identifisere en bruker. Lagring av disse opplysningene kunne til en viss grad ha avhjulpet utfordringen med at de store private nettverksløsningene ikke er underlagt lagringsplikten, men det ville samtidig ha økt personverninngrepet og kravet til nødvendighet. Den teknologiske utviklingen går imidlertid nå så fort at behovet for lagring av destinasjonsdata kan bli aktuelt i nær fremtid. I denne omgang bør det således ikke utelukkes at lagringsplikten i fremtiden skal kunne utvides til å omfatte data på destinasjonssiden. Det vises til det som er sagt ovenfor om teknologinøytralitet.

Kripos mener videre at tildelingstidspunktet for IP-adressen må omfattes av lagringsplikten. Det vil si at når politiet ber om det må det være mulig å få svar på hvor lenge den aktuelle IP-adressen har vært tildelt abonnenten. Selv om IP-adresser kan ha en dynamisk tildeling er det ikke uvanlig at samme IP-adresse blir benyttet av samme abonnent i lang tid og det er grunn til å tro at dette ikke blir mindre vanlig dersom det i fremtiden ikke blir samme mangel på IP-adresser som i dag.

7.3.3 Lagringssted

Kripos har ingen sterke meninger om hvor de aktuelle dataene skal lagres, men det må føres en oversikt over hvor politiet kan finne de dataene som lagres. En slik oversikt må inneholde kontaktpunkter for hvor politiet skal henvende seg for å hente ut data.

Det må videre stilles krav til hvordan utvekslingen med politiet skal skje og at denne skal kunne skje på en sikker måte. Dette enten med hver enkelt tilbyder, hvert enkelt lagringssted eller gjennom et felles grensesnitt som blir satt opp av tilbyderne.

Uthenting av data bør skje sentralt i politiet slik at ikke hvert politidistrikt skal måtte forholde seg til flere hundre tilbydere med forskjellige grensesnitt, og tilhørende utfordringer med administrasjon av kryptonøkler på begge sider.

7.4 Lagringstid

Kripos mener at lagringstiden må være tolv måneder. Dette utgangspunktet hadde Kripos også i høringsuttalelsen til implementeringen av DLD. I høringsuttalelsens til implementeringen av DLD punkt 5.1.1 går Kripos gjennom åtte forhold som begrunner behovet for en lagringstid på tolv måneder. Det vises til denne gjennomgangen, som fortsatt er relevant.

Behovet som underbygger denne lagringstiden har ikke blitt mindre i tiden som har gått, snarere tvert imot. Ofte vil det kreve en omfattende etterforskning for å skaffe til veie informasjon om nettaktivitet. Gjennomgangen av beslaglagte telefoner og datamaskiner tar lang tid og underveis er det behov for bruk av tvangsmidler som ransaking, beslag og utleveringspålegg for å få tilgang til data som kan si noe om vedkommendes aktivitet.

Internett er globalt og det vil som regel være behov for rettsanmodninger om utlevering av informasjon fra utenlandske nettsteder. Det kan her nevnes at en rettsanmodning til USA om innhenting av data fra en tilbyder av innholdstjenester vil kunne ta opptil tolv måneder. Selv om dataene som amerikanske tjenestetilbydere har om europeiske brukere skulle bli flyttet til Europa er det grunn til å tro at det vil ta flere måneder å få ut data gjennom en rettsanmodning. Stadig mer av kommunikasjonen i Norge skjer over internett gjennom utenlandske tjenestetilbydere, noe som gjør at behovet for å hente ut data gjennom rettsanmodninger er økende.

En gjennomgang av mistenktes kommunikasjonsenhet forutsetter at politiet faktisk får tilgang til enheten som skal undersøkes. Avanserte tilgangsløsninger og kryptering blir mer og mer vanlig og det tar ofte lang tid før politiet kan starte på selve gjennomgangen. Også dette underbygger behovet for lagringstid i tolv måneder.

7.5.1 Materielle vilkår for utlevering

Det er i dag ikke særskilte strafferammekrav ved utlevering av opplysninger om tildelte IP-adresser for utførelse av politiets oppgaver i eller utenfor etterforskning.

Kripos er enig i at nyere praksis fra EMD og EØS-retten som der det innføres en lagringsplikt med begrunnelse i kriminalitetsbekjempelsen setter krav til at opplysningene bare kan utleveres når det gjelder alvorlig kriminalitet. Lagring av opplysninger som kan identifisere abonnenter bak IP-adresser er imidlertid ikke et så stort inngrep som lagring av de trafikkdata som var ment lagret i medhold av DLD. Dette tilsier at et eventuelt strafferammekrav bør ligge klart lavere for utlevering av abonnementsopplysninger for IP-adresser i forhold til andre data som var men lagret ved DLD.

Departementet foreslår at strafferammekravet bør være på minst ett eller to års fengsel, eventuelt i kombinasjon med særskilte angitte straffebud.

Ved bruk av tvangsmidler som beslag, ransaking og utleveringspålegg kan politiet få tilgang til svært personsensitivt materiale med strafferammekrav som ligger langt under det som foreslås for å hente ut abonnementsdata. Sett hen til vilkårene for bruk av tvangsmidler stiller Kripos spørsmål ved om ikke strafferammekravet bør ligge lavere enn det departementet foreslår. Dersom lovgiver likevel skulle komme til at det må være et strafferammekrav som foreslått i høringsnotatet mener Kripos at dette ikke bør overstige ett år. Innenfor en strafferamme på ett år så er kriminaliteten alvorlig nok til å forsvare utlevering av de lagrede

opplysningene også i medhold av den praksis departementet har vist til etter EMK og EØS-retten. Ved å velge et strafferammekrav på ett år vil det ikke være behov for å nevne enkelte straffebud særskilt.

Dersom departementet velger et strafferammekrav på to år, kombinert med særskilte angitte straffebestemmelser, bør etter vår vurdering mange bestemmelser med strafferamme på ett år tas inn i bestemmelsen, siden disse i seg selv representerer kriminalitet som er alvorlig nok til å innhente slike opplysninger etter praksis i EMD eller etter EØS-retten. Identifisering av brukere av IP-adresser kan ha betydning for etterforskningen av nær samtlige slike forhold.

Kripos er enig med departementet i at det ikke bør skilles mellom utlevering av opplysninger til etterforskning og utlevering til forebygging av tilsvarende kriminalitet.

Slik Kripos forstår høringsnotatet foreslås det ikke endringer i ekomloven § 2-9, 3. ledd. Denne adgangen til utlevering av abonnementsopplysninger vil således bestå for data som ikke er lagret i medhold av ny § 2-8a. Politiet vil således etter den bestemmelsen fortsatt ha adgang til å få utlevert abonnementsinformasjon, også hva gjelder IP-adresser, i den grad disse er lagret med en annen begrunnelse enn den nye lagringsplikten.

Abonnementsinformasjon vil være viktig for politiets virksomhet utover i forebygging og etterforskning, herunder eksempelvis redningsarbeid eller søk etter savnede personer. Dersom det nå innføres en lagringsplikt er det en klar mulighet for at lagring av IP-abonnementsinformasjon av andre grunner vil gå ned i omfang eller opphøre. Lagringsplikten, kombinert med den teknologiske utviklingen, vil da kunne medføre at politiet i fremtiden vil få tilgang til mindre informasjon enn i dag og at dette gjør blant annet politiets søk- og redningsarbeid vanskeligere. Det bør på bakgrunn av dette vurderes om det kan innføres en særregel om uthenting av abonnementsinformasjon lagret etter ny § 2-8a til bruk i søk- og redning, som i alle fall sikrer politiet tilgang til informasjon i samme grad som i dag.

7.5.2 Utlevering av informasjon med utgangspunkt i både IP-adresse og abonnement

Kripos støtter forslaget om at det skal være mulig å innhente lagrede opplysninger både med utgangspunkt i en IP-adresse og et abonnement og tiltrer departementets begrunnelse for dette.

7.5.3 Prosessuelle regler

Det er i dag ikke noe krav om at utlevering av abonnementsopplysninger knyttet til IP-adresser fordrer påtalemessig beslutning, rettslig kjennelse eller særskilt vedtak fra NKOM som fritar fra taushetsplikt.

Når det nå innføres en lagringsplikt for tilbyderne av internettaksess vil politiet kunne få tilgang til noe mer data enn etter dagens regler. Likevel er ikke dette data av en så inngripende karakter for den enkelte at det fordrer særskilte prosessuelle garantier ved utlevering. Kripos er enig i departementets vurdering av praksis fra EMD og EU-domstolen på dette området og støtter forslaget om at dagens utleveringspraksis videreføres.

Kripos støtter videre at det ikke er behov for endringer i regelverket rundt behandling av disse opplysningene når de er kommet til politiet. Reglene i politiregisterloven og straffeprosessloven, samt det kontrollregimet som er lagt rundt politiets behandling av personopplysninger i og utenfor straffesak, er tilstrekkelige for en forsvarlig behandling av også disse opplysningene.

7.6 Bruk av opplysninger om IP-adresser i sivile saker

Tvisteloven § 22-3 setter den bevisforbud for taushetsbelagte opplysninger, men unntakene gir muligheter for at beviset likevel kan føres dersom taushetsplikten oppheves av NKOM eller retten etter en konkret vurdering. I disse vurderingene kan det tas hensyn til hva som er begrunnelsen for at dataene eksisterer.

KAPITTEL 10 - KOSTNADSFORDELINGSMODELL

Kripos klare utgangspunkt er at kostnader knyttet til lagring, herunder investering i og drift av løsninger, må dekkes av tilbyderne selv. Kriminalitetsbekjempelse er et sentralt samfunnsmessig hensyn, og staten bør som det helt klare utgangspunkt kunne pålegge næringer tilretteleggingskrav uten kompensasjon. Kripos kan ikke se at dette tilfellet skiller seg nevneverdig fra for eksempel situasjonen for finansnæringen, som selv er pålagt å dekke kostandene knyttet til hvitvaskingsregisteret. En utvikling i retning av at staten skal måtte betale virksomheter for å legge til rette for ivaretakelsen av grunnleggende samfunnsmessige behov og tjenester, er etter vår oppfatning klart uheldig.

Departementet foreslår fem alternative kostnadsfordelingsmodeller. I alle modellene er kostnadene delt i tre; investeringskostnader, faste driftskostnader og uthentingskostnader. I alle modellene er det lagt til grunn at staten skal dekke uthentingskostnadene, og modellene skiller for øvrig på hvor mye, om noe, staten skal dekke av investerings- og/eller driftskostnader.

Kripos mener at skillet mellom investeringskostnader og faste driftskostnader kan fremstå som kunstig og at det i hvert fall er svært vanskelig å rubrisere kostnadene riktig. Et eksempel kan være leasing i stedet for innkjøp av serverpark. Er dette investering eller drift? Kripos er bekymret for at valg av en modell der det skilles mellom investerings- og driftskostnader kan medføre en migrering av kostnader mellom de to postene alt etter hvor staten dekker mest.

Dersom det velges en løsning hvor staten skal dekke annet enn rene uthentingskostnader, foreslår Kripos således en modell hvor det ikke skilles mellom investerings- og driftskostnader, jf modell E.

Departementet ber om høringsinstansenes syn på om en fordelingsnøkkel bør være lik for tilbyderne eller om den kan være individuelt tilpasset. Kripos mener at en fast fordelingsnøkkel klart er å foretrekke. Det er flere hundre tilbydere og inngåelse av individuelle refusjonsavtaler med disse og en etterfølgende individuell kostnadskontroll fremstår som et unødvendig dyrt og byråkratisk system som det vil være krevende å drifte.

Det varierer fra land til land hvor mye av kostnadene til datalagring som dekkes av staten. I England dekker staten alle utgifter. I Finland dekkes 2/3 av staten, mens tilbyderne dekker resten uten at politiet må betale for hver enkelt uthenting. Hvor stor andel av investerings- og driftskostnader som bør betales av staten er vanskelig å tallfeste. Det er imidlertid klart at dersom teletilbyderne skal ha et insentiv til kostnadseffektive løsninger, så må teletilbyderne dekke en klart følbar del av utgiftene.

Velges en modell med statlig kompensasjon, som samtidig legger opp til at uthentingskostnader skal belastes politiet, mener Kripos (subsidiært) at tilbyderne i hvert fall må dekke en større del av investerings- og driftskostnader enn staten.

Når det gjelder uthentingskostnader bør disse begrenses til å inneholde rene kostnader med å hente ut lagrede data og overføre disse til politiet. Utover personellkostnader kan ikke Kripos se at det kan være snakk om store kostnader, da investering og faste driftskostnader med lagringen skal holdes utenfor, samt at det er vanskelig å se for seg en lagringsløsning hvor selve uthentingen av data medfører store investeringer eller driftskostnader. Automatiseringsløsninger kan selvsagt endre på dette bildet, men det bør som departementet skriver utredes nærmere mellom politiet og tilbyderne/NKOM.

Det helt sentrale for politiet er at valget av kostnadsfordelingsmodell ikke får noen innvirkning på om politiet faktisk velger å innhente slike data i den konkrete sak. Det vil særlig være den lokale kostnadsbelastningen for uthenting av data som vil kunne påvirke dette. Dette taler for en relativt lav stykkpris for hver henvendelse kombinert med en sentralisert finansieringsordning.. Det kan her nevnes at det i Sverige opereres med en stykkpris på 150 kroner i kontortiden og 170 kroner utenfor kontortid.

Avslutningsvis vil Kripos understreke at valget av kostnadsmodell for lagring og uthenting av IP-informasjon ikke må lage utfordringer for de innarbeidede ordningene som gjelder innhenting av trafikkdata og tilrettelegging for kommunikasjonskontroll.

KAPITTEL 11 - ØKONOMISKE OG ADMINISTRATIVE KONSEKVENSER

Økt lagring av IP-informasjon vil medføre at politiet vil hente ut mer data enn i dag, noe som igjen vil medføre høyere kostnader for politiet i en modell der politiet dekker uthentingskostnadene. Dersom betalingsmodellene som benyttes i dag videreføres vil økningen i uthentingskostnader alene bli betydelig. Med den stramme økonomien som er i politiet er Kripos redd for at valget om politiet skal innhente IP-informasjon kan bli et spørsmål om hensynet til økonomi snarere enn hensynet til forebygging/etterforskning. Det må således sørges for en sentral finansiering av økte uthentingskostnader før regelverket trer i kraft.

Tilsvarende må det på plass finansiering for en statlig løpende ordning for kostnadskontroll og refusjon av investerings- og driftsutgifter for teletilbyderne.

I dag forvalter Kripos avtalene med tre tilbydere når det gjelder innhenting av trafikkdata og tilrettelegging for kommunikasjonskontroll. Når en ordning med lagring av IP-informasjon innføres må det inngås avtaler med flere hundre aktører som tilbyr offentlig tilgang til internett. Kripos har innenfor dagens organisasjon ingen mulighet til å løse dette oppdraget og mener at inngåelse og forvaltning av disse avtalene må skje sentralt i politiet

I tillegg til investeringer og driftsutgifter hos tilbyderne vil mottak av IP-informasjon fra flere hundre tilbydere medføre behov for investeringer og driftsutgifter på politiets side. Selv med en løsning hvor staten dekker deler av \ investeringskostnadene for tilbyderne vil det trolig bli valgt flere forskjellige lagringsløsninger som har ulike format på informasjonen som hentes ut

og som ikke har ett felles grensesnitt mot politiet. Arbeidet med mottak av data og kvaliteten på disse henger tett sammen med forvaltningen av avtalene med tilbyderne og bør også skje sentralt i politiet.

Med hilsen

Ketil Haukaas
assisterende sjef Kripos

Saksbehandler:
Håvar Undeland
politiadvokat
Telefon: 909 42 152

Vedlegg:
- Høringssvar – datalagringsdirektivet – 12.10.2010
- Høringssvar – datalagringsforskriften – 10.04.2012
- Høringssvar – tiltak 14 JD's IKT strategi – 11.01.2016
- Høringssvar - tiltak 15 JD's IKT strategi – 08.02.2016

POLITIET

Politidirektoratet
Postboks 2090 Vika
0125 Oslo

Politiets utlendingsenhet

Deres referanse:	Vår referanse:	Dato:
	20/156108 - 2	18.01.2021

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

Det vises til brev av 11.12.2020 fra Politidirektoratet (POD) vedlagt høringsbrev av 09.10.2020 fra Kommunal- og moderniseringsdepartementet og Justis og beredskapsdepartementet om forslag til endringer i lov av 04.07.2003 nr. 83 om elektronisk kontroll (ekomloven). Frist for innspill til høringen er satt til 18.01.2021.

Endringsforslaget innebærer både innføring av en plikt for tilbydere av ekomtjenester til å lagre IP-adresser, og en avgrenset rett for politiet til å få tilgang til IP-adresser med det formål å forebygge og etterforske alvorlig kriminalitet. Departementene ønsker særlig tilbakemelding på hvilket strafferammekrav som bør oppstilles, og på hvor lang lagringstiden bør være.

PU har et nasjonalt ansvar for registrering av alle asylsøkere, undersøkelse av asylsøkernes reiserute, fastsette identiteten til utlendinger og iverksette alle negative vedtak i asylsaker, jf. Instruks for PU av 1.mai 2005 og POD rundskriv 2012-005. PU er ikke tillagt påtalekompetanse, og har derfor heller ikke adgang til å etterforske straffesaker.

PU har ingen kommentarer til de rettslige vurderingene som departementet begrunner innstramming i utleveringsadgangen med, der ivaretakelse av kravet til proporsjonalitet etter Grunnloven, EMK og kommunikasjonsverndirektivet står sentralt. PU ønsker likevel å kort bemerke at siden lovendringsforslaget vil innebære at utlevering kun kan skje når det er nødvendig for å forebygge eller etterforske en handling som kan innebære straff av fengsel i x år eller mer, alternativt i kombinasjon med unntak for spesifikke straffebud, så vil dette medføre at det ikke vil være anledning for PU å få utlevert IP-adresser med formål i ovennevnte ansvarsområder.

Etter gjeldende bestemmelse i ekomloven § 2-9 tredje ledd så gjelder unntaket for taushetsplikten, som også omfatter opplysninger om abonnenters disponering av IP-adresser, alle oppgavene politiet utfører, herunder sivile gjøremål, med mindre det foreligger særlige forhold som gjør det utilrådelig å etterkomme en utleveringsanmodning. Det vises her også til pkt. 3 i høringsbrevet der gjeldende rett er omtalt. PU har således etter gjeldende rett begrenset hjemmel til å innhente IP-adresser.

Blant PUs primære ansvarsområder er som nevnt over avklaring av ID og reiserute, samt sikre effektuering. Innhenting av IP-adresser fra tilbydere er imidlertid ikke et aktuelt verktøy i dette arbeidet. Ivaretakelse av PUs kjerneoppgaver tilsier således ikke behov for at PU fortsatt har hjemmel for innhenting av IP-adresser.

Selv om PU ikke har påtalekompetanse og således ikke kan utføre etterforskingsskritt, så har PU som politiorgan en plikt til å bidra med å forebygge kriminalitet og andre krenkelser av den offentlige orden og sikkerhet, samt avdekke og stanse kriminell virksomhet jf. politiloven § 2 nr. 2 og 3. PU skal bearbeide og analysere relevant informasjon innenfor vårt felt og informere rett politimyndighet om personer som antas å tilhøre kriminelle nettverk eller antas å ha begått alvorlige straffbare handlinger, herunder terrorhandlinger og krigsforbrytelser, jf. Instruks for PU av 01.06.05.

Det er også på grunn av dette viktig at politidistriktene, PST og Kripos har tilstrekkelig gode verktøy til å etterforske og iretteføre saker som treffer utlendingsfeltet.

På side 35 i høringsbrevet ber departementene om høringsinstansenes syn på hvilket strafferammenivå som bør settes. PU har ingen kommentarer når det gjelder de straffebud som nevnes, utover å påpeke at alle straffebudene verner om viktige samfunnsinteresser og politiet bør derfor ha best mulig verktøy for å kunne etterforske mulige lovbrudd.

Når det gjelder straffebud på utlendingsfeltet så fremkommer det av utlendingsloven § 108 at overtredelse av fjerde og femte ledd har strafferamme på hhv inntil 3 og 6 års fengsel (menneskesmugling og hjelp til ulovlig opphold). Forebygging og etterforskning av handlinger som omfattes av disse bestemmelsene vil således etter de foreslåtte endringer utløse rett til innhenting av IP-adresser.

Utlendingsloven § 108 tredje ledd gir regler om straff for bruk av ulovlig arbeidskraft, utilbørlig utnyttelse av en utlendings situasjon, rettstridig forleding av en utlending til å reise inn i riket med sikte på å bosette seg der, overlatelse av reisedokumenter mm som kan bli brukt til innreise, og brudd på ilagt innreiseforbud etter en utvisning. Strafferammen for brudd på disse bestemmelsene er bot eller fengsel inntil to år. Dette er straffebud som verner om viktige samfunnsinteresser der det ikke vil være anledning til å innhente IP-adresser dersom det settes et generelt strafferammekrav på minimum 2 år.

Videre nedfeller utlendingslovens § 108 annet ledd bokstav a blant annet straff for ulovlig opphold og unndratt effektuering (jf. henvisning til § 55 første og andre ledd og § 90 sjette ledd). Strafferammen er bot og/eller fengsel i inntil seks måneders fengsel. Det antas at mulighet for innhenting av IP-adresser vil kunne være et nyttig verktøy for å avdekke ulovlig opphold, herunder oppholdssted.

Sett i lys av straffebudene i utlendingslovens § 108 andre og tredje ledd, samt de straffebud som departementene trekker frem på side 35, mener PU at det generelle strafferammenivået

bør være på minimum et år, samt at det foretas en vurdering av om nevnte straffebud i utlendingsloven § 108 annet ledd også skal omfattes spesifikt.

Når det gjelder varigheten av lagringsplikten så har PU ingen særskilte synspunkter.

Med hilsen

Kristel Lee Høgslett **Rolf Odner**
Seksjonsleder *Politiadvokat 2*

Dokumentet er elektronisk godkjent uten signatur.

Kopi:
Kristel Lee Høgslett
Rolf Odner

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 strømenn 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