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