



POLITIET

Samferdselsdepartementet

postmottak@sd.dep.no

Deres referanse
12/2062

Vår referanse
201300738

Dato
6. juni 2013

Høringsuttalelse - forslag til regler om kostnadsfordeling, nødrettssituasjoner og taushetsbelagte data

Det vises til Samferdselsdepartementets høringsbrev av 26. april 2013, med vedlagt høringsnotat.

Kostnadsfordeling

Kripos deltok i Kostnadsfordelingsutvalget som leverte sin rapport 1. februar 2012. Gjennom arbeidet i utvalget og den etterfølgende høringsrunden har Kripos' generelle innspill til kostnadsfordelingsmodeller kommet godt frem.

Det har i utvalget og i høringsrunden vært særlig viktig for Kripos å oppnå en kostnadsløsning som sikrer at det er dataenes verdi som etterforskningsmateriale, og ikke kostnadene ved innhenting, som avgjør om slik innhenting rent faktisk skjer. Den ordning som departementet nå foreslår, hvor statens dekning av utgifter til lagring og uthenting skal ta utgangspunkt i tilbyders antall abonnenter, synes å legge til rette for en slik løsning.

Til den foreslåtte løsning vil vi også bemerke at det for politiet vurderes å være en klar fordel at antall etablerte databaser for lagring av DLD-data holdes så lavt som mulig. Departementet uttaler at størrelsen på kostnadsdekningen vil ta utgangspunkt i etablering av to sentrale baser. Vi støtter en slik løsning og understreker betydningen av at man ved fastsettelse av kostnadsdekningens størrelse i tilstrekkelig grad ihensyntar de incitamenter som ligger her i forhold til tilbydernes valg av lagringsløsninger.

For øvrig hva gjelder kostnadsfordelingsspørsmålet tillater vi oss å vise til våre innspill til kostnadsfordelingsutvalgets rapport, jf vedlagte skriv av 16. april 2012.

Kort om behovet for overgangsregler

Det legges nå opp til at datalagringsdirektivet skal tre i kraft i Norge 1. januar 2014, og at lagringsplikten iverksettes fra januar 2015. Kripos mener at de stadige utsettelsene av ikrafttredelsen fordrer at det blir innført overgangsordninger som sikrer at politiet får tilgang til DLD-data også i perioden frem til iverksettelse.

Kripos

Den nasjonale enhet for bekjempelse av organisert og annen alvorlig kriminalitet
Brynsalléen 6, Postboks 8163 Dep, 0034 OSLO
Tlf: 23 20 80 00 Faks: 23 20 88 80
E-post: kripos@politiet.no

Org.nr.: 974 760 827

Historisk har politiet hatt anledning til å hente ut trafikkdata fra teletilbyderne i straffesaker der disse har hatt betydning som bevis. Dataene har reelt sett vært en utlissing fra teletilbydernes fakturerings-system. Det blir nå stadig mer vanlig med betalingsløsninger som reduserer tilbyders behov for lagring av data for slike administrative formål. Dette har blant annet som konsekvens at tilbyders plikt til å slette, etter dagens regelverk, inntreffer på et langt tidligere tidspunkt. Dette følges opp av Datatilsynet. TeliaSonera og Telenor opplyser at de nå lagrer historiske trafikkdata i 90 dager. Dette er den maksimale lagringstiden som Datatilsynet tillater ved månedlig fakturering. Ved kvartalsvis fakturering, som var vanlig tidligere, kan data lagres i 5 måneder. For IP-adresser er dagens lagringstid 21 dager.

Et av direktivets formål har nettopp vært å sikre datatilgang uavhengig av tilbydernes eget lagringsbehov. Som ovennevnte viser har utsatt iverksettelse store konsekvenser for omfanget av politiets tilgang og derigjennom våre muligheter til å sikre viktige bevis i alvorlige straffesaker. Det er over to år siden en lagringstid på 6 måneder ble lovfestet og det foreligger nå også en forskrift som regulerer nærmere lagringsplikt og tilrettelegging. I lys av dette, og hensett til de utfordringer utsettelsene reiser for politiet, bør det legges til rette for ordninger som avhjelper ulempene ved sen iverksettelse.

Nødrett

Kripos' vil innledningsvis bemerke at det for oss fremstår som noe usikkert om en lovfesting av dagens nødrettsinstitutt er nødvendig. Departementet har pekt på at en egen bestemmelse vil synliggjøre politiets rett til uthenting og bidra til større forutberegnelighet. Slike følger forutsetter, etter Kripos' vurdering, at den bestemmelse som foreslås ikke bidrar til en innskrenking av dagens praksis. Nødrett er et innarbeidet institutt i norsk rett, og en kodifisering må ikke medføre et nødrettsbegrep med et annet innhold enn det som følger av tradisjonell nødrettslære. Kripos har med dette utgangspunktet funnet grunn til å kommentere deler av forslaget i høringsnotatet.

Gjeldende rett

Under gjeldende rett pkt 3.2.3 er det i høringsnotatet skrevet noe om hva som er situasjonen når politiet iverksetter kommunikasjonskontroll med hjemmel i nødrett. Kripos forstår departementet slik at det er lagt inn en forutsetning om at det foreligger en nødssituasjon i det som er skrevet om kommunikasjonskontroll.

For ordens skyld finner Kripos grunn til å presisere at det enten må det foreligge en reell nødrettssituasjon eller så må vilkårene etter straffeprosessloven være oppfylt, for at politiet skal kunne iverksette kommunikasjonskontroll. I gråsonen mellom redningsarbeid og etterforskning kan situasjonen være at det ikke foreligger hjemmel for bruk av kommunikasjonskontroll etter straffeprosessloven. I slike tilfeller kan nødrett være aktuelt, men da bare dersom det rent faktisk foreligger en reell nødsituasjon, herunder at denne er pågående eller nært forestående.

I høringsnotatet på side 23, øverste avsnitt, er det beskrevet nærmere hvilket kontrollregime kommunikasjonskontroll er underlagt, dersom den iverksettes uten forhåndsgodkjennelse fra domstolen. Kripos finner her grunn til å presisere at denne beskrivelsen ikke er treffende for situasjonene der kommunikasjonskontroll er iverksatt med hjemmel i nødretten.

Kommunikasjonskontroll som er iverksatt med hjemmel i nødretten er ikke underlagt etterfølgende domstolskontroll. All bruk av kommunikasjonskontroll i etterforskningssporet

skal rapporteres til riksadvokaten uavhengig av hjemmel for metodebruken. Kommunikasjonskontroll iverksatt med hjemmel i nødretten utenfor etterforskningssporet skal ikke rapporteres. Det kan her vises til riksadvokatens bemerkninger til Kommunikasjonskontrollutvalgets årsrapport fra 2009, inntatt i riksadvokatens skriv av 7. september 2010 samt til riksadvokatens skriv av 1. oktober og 3. november 2009.

Utforming av bestemmelsen

Kripos støtter departementets forslag til ordlyd hva gjelder knytningen mellom person og kravet til fare for «...liv og helse...». Samtidig mener vi det er en klar svakhet ved forslaget at man har innskrenket bestemmelsen til kun å gjelde personer, i forhold til den generelle nødrettsbestemmelsen i straffeloven som også omfatter andre rettsgoder som befinner seg i en nødssituasjon. For Kripos fremstår denne innskrenkingen som ubegrunnet.

Nødrettssituasjoner vil i normaltilfellene knytte seg til personers liv eller helse, men man kan også tenke seg situasjoner hvor andre rettsgoder er i fare, og hvor man har et klart behov for trafikkdata for å kunne verne disse.

Et eksempel på dette kan være anslag mot rikets sikkerhet, og det vises her til uttalelser fra Lundkommisjonen (Lundkommisjonens rapport side 304):

... ”Men kommisjonen utelukker ikke at det kan foreligge helt spesielle situasjoner der bruk av slike etterforskningsmetoder [ulovhjemlede j.s.] kan forsvares med nødrett når dette er eneste utvei for å hindre alvorlige – eller fortsatt alvorlige – anslag mot rikets sikkerhet.”

Et annet eksempel kan være nødvendigheten av å finne en adresse til en datamaskin som blir brukt til å angripe viktige samfunnsgoder og kritisk infrastruktur.

I praksis vil man kanskje ofte være kommet over i etterforskningssporet i disse tilfellene, slik at påtalemyndighetens hastekompetanse kan benyttes, men Kripos kan ikke se noen god begrunnelse for å begrense nødrettshjemmelen til kun å gjelde tilfeller der personers liv og helse er i fare.

Praktisering av bestemmelsen

I høringsnotatet pkt 3.3.4 foreslår departementet en ordning med opprettholdelse av innhentede data uthentet i nødrettssporet, der nødsituasjonen går over i en etterforskning. Dette er Kripos uenig i.

Kripos kan ikke se at dette er godt begrunnet. Den nye nødrettsbestemmelsen i ekomloven § 2-9a, vil være en særskilt hjemmel for innhenting av trafikkdata i nødssituasjoner. Dersom vilkårene for å hente inn trafikkdata etter § 2-9a er tilstede, og denne hjemmelen benyttes, vil innhentingen være lovlig gjennomført. I den alminnelige nødrettslæren er det klart at en handling som er gjennomført i tråd med nødretten fullt ut er rettmessig, jfr. Matningsdal og Bratholm, Straffeloven Kommentartutgave, 2. utgave, s. 375. Kripos kan ikke se at det er behov for at en slik fullt ut rettmessige handling, nemlig en lovlig innhenting hjemlet i § 2-9a, skal måtte opprettholdes av påtalemyndigheten og deretter underlegges domstolskontroll fordi situasjonen har beveget seg fra en fase over i en annen.

I straffeprosessloven finnes det regler om tvangsmidler som krever opprettholdelse av påtalemyndigheten etter at de er gjennomført. Dette er tvangsmidler som kan utføres av

polititjenestemenn uten påtalemyndighet (eller enhver på ferske spor). Opprettholdelsen inngår i slike tilfeller i påtalemyndighetens kontrollfunksjon. Vi kan vanskelig se at det foreligger et tilsvarende behov for kontroll her, hvor primærkompetansen for utlevering i nødrettstilfellene er foreslått lagt til politimesteren.

Vi vil til dette samtidig bemerke at vi prinsipielt mener kompetansen for uthenting i nødrettssituasjoner bør legges på et nivå tilsvarende det som vil gjelde ved hastesituasjoner i etterforskning utenfor nødrettssporet. En slik løsning vil etter vår oppfatning samsvare bedre med den praksis som har utviklet hva gjelder beslutningskompetanse i nødrettssporet. I en ordinær etterforskning kan som kjent utlevering av trafikkdata i dag besluttes av påtalemyndigheten.

Etterfølgende kontroll.

I høringsnotatet legger departementet opp til at det skal innføres en ordning med etterfølgende kontroll av politiets bruk av nødrettsbestemmelsen for utlevering av trafikkdata. Kripos mener en slik ordning er unødvendig, da det allerede finnes tilstrekkelige kontrollfunksjoner i politi og påtalemyndighet.

Bruk av nødrettshjemmelen i etterforskingssporet vil ikke bli omfattende. Det er opplyst at 80% av dagens henvendelser kommer fra HRS. Resten kommer fra politidistrikter og særorgan, og også disse resterende 20% må antas å ha et stort innslag av redningsaksjoner. Man står da igjen med et svært lite antall hvor faren for omgåelse av regelverket er aktuell. Kripos kan ikke se at det er fremkommer noe i høringsnotatet som gir grunnlag for å underlegge disse få sakene et eget kontrollregime. Forslaget fremstår derfor som ubegrunnet.

Med unntak av de mest inngripende tvangsmidlene, som kommunikasjonskontroll og romavlytting, er ikke bruk av tvangsmidler underlagt kontroll utover den interne kontroll som ligger i påtalemyndighetens system, eller den domstolskontroll som blir foretatt ved at straffesakene føres for retten. Tvangsmidler som ransaking (ved bruk av hasteskompetanse) og beslag er ikke i seg selv tvangsmidler som er underlagt særskilt kontroll, ei heller der hjemmelsgrunnlaget er nødrett.

I følge forslaget til ny regel skal beslutningen om utlevering av trafikkdata i nødrettstilfellene fattes av politimester. Dette vil i seg selv gi en utvidet kontroll i forhold til alminnelig bruk av tvangsmidler. Selv om man skulle legge beslutningskompetansen til påtalemyndigheten, vil det ligge en kontroll i at påtalemyndigheten faktisk må fatte en begrunnet beslutning i nødrettstilfellene. Dette er kontrolloppgave som ligger i kjerneområdet for påtalemyndighetens funksjon.

Kripos ser at det kan være et behov for å følge utviklingen i bruken av nødrett som hjemmel for utlevering av trafikkdata. Bruk av nødrett som hjemmel bør således, i hvert fall i en overgangsperiode, rapporteres til overordnet myndighet. Ettersom det i stor grad vil dreie seg om utlevering av trafikkdata i redningsaksjoner, antar en at POD kan være en aktuell adressat hva gjelder politiets bruk.

Dersom man velger å innføre en ordning hvor et eksternt organ fører tilsyn, bør en slik oppgave tillegges et allerede eksisterende organ. Kontrollutvalget for kommunikasjonskontroll (KK-utvalget) har lang erfaring med å kontrollere tvangsmiddelbruk fra politiet. Vi bemerker at en slik eventuell kontrolloppgave vil være

ressurskrevende. Det følger av høringsnotatet at teletilbyderne mottar ca. 1200 nødrettsanmodninger i året.

Signaleringstrafikk, PUK-koder og kundereskontro

Signaleringstrafikk

I lovforslaget avgrenses det mot signaleringstrafikk. Dette er en type data som bl.a. kan hjelpe politiet til å geografisk plassere et kommunikasjonsanlegg, eksempelvis en mobiltelefon. Datatypen er svært viktig for politiet ved bruk av kommunikasjonskontroll.

Kripos har ved flere anledningen fremmet behov for en generell lovhjemmel knyttet til lokalisering av bl.a. mobiltelefoner. Vi sikter da til en hjemmel som ikke nødvendigvis må knyttes til kommunikasjonskontroll og som ikke er avhengig av at telefonen kommuniserer. I Kripos' høringsuttalelse til Metodekontrollutvalget ble det understreket at en slik hjemmel burde utformes så teknologinøytralt som mulig, slik at ikke innhenting av posisjonsdata ble begrenset til kun å gjelde situasjonene hvor man bruker IMSI-catcher (straffeprosessloven § 216b, 2. ledd, bokstav c).

Regjeringen lanserte 17. desember 2012 «Nasjonal strategi for informasjonssikkerhet». Sammen med denne strategien ble det lansert en handlingsplan hvor flere strategisk viktige tiltak er inntatt. Ett av tiltakene er:

Tiltak 5.5: Utrede mulighet for bedre sanntidsposisjonering av mobile kommunikasjonsenheter

Bakgrunn: Mer nøyaktig posisjonering av mobile kommunikasjonsenheter er nødvendig i situasjoner hvor det er viktig å gripe inn raskt. Politiet kan i dag få tilgang til posisjoneringsdata med hjemmel i straffeprosessloven § 216b. Det er behov for en lovendring som gir adgang til å spore mobile kommunikasjonsenheter på en mer nøyaktig måte, også på tidspunkter der kommunikasjonsenheten ikke aktivt benyttes til kommunikasjon.

Tiltak: Det skal foretas en utredning om bruk av sanntidsposisjonering for etterforskning av alvorlige straffesaker og i redningsoperasjoner der liv og helse er i fare. Utredningen skal også vurdere om tilbyderne skal pålegges en leveringsplikt av posisjoneringsdata og hvilke type data som skal utleveres. Både hensynet til kriminalitetsbekjempelse og personvern skal ivaretas.

Ansvarlig departement: JD

Dette tiltaket synes å gå rett til kjernen i den problematikken som ble tatt opp i Metodekontrollutvalget og høringen rundt kommunikasjonskontroll for å avdekke oppholdssted. Kripos mener det foreligger et klart behov for at det innføres en generell regel om sanntidsposisjonering av mobile kommunikasjonsenheter i Norge. Det kan her nevnes at man i Danmark har valgt å innføre en slik hjemmel i retsplejelovens § 791a.

Også historiske data av denne typen kan være til stor hjelp for politiet. Ofte blir ikke politiet koblet inn før etter at den aktuelle straffbare handling er begått, f.eks ved drap eller voldtekter. Behovet for tilgang til, og dermed lagring av, denne type data vil i mange tilfeller

være like stort som ved historiske trafikkdata, særlig ettersom genereringen av denne datatypen ikke fordrer abonnentens aktive bruk av kommunikasjonsanlegget.

Slike data lagres i dag i 10 til 14 dager. Kripos mener at dette tidsrommet er alt for kort, og mener gode grunner taler for å lagre denne datatypen på lik linje med trafikkdata. Det opplyses i høringsnotatet at Samferdselsdepartementet eventuelt vil komme tilbake til spørsmålet om lagring av slike data. Kripos vil her understreke behovet for at en slik lagringsplikt faktisk blir vurdert.

PUK-koder og kundereskontro

Det prinsipielle utgangspunktet til Kripos er at PUK-koder ikke omfattes av taushetsplikten i ekomloven. Det vises her til den juridiske betenkningen som ble uarbeidet av Ørnulf Røhnebæk i 2008. Selv om PUK-koden kan benyttes til å åpne låste sim-kort hvor det kan ligge informasjon som er taushetsbelagt hos teletilbyder, er den praktiske realitet at dette skjer etter at sim-kortet (og dermed dataene) er tatt i beslag av politiet.

Sett bort fra den prinsipielle uenigheten, mener vi den løsning som foreslås for politiets tilgang til kodene representerer en praktisk og god tilnærming. Kripos støtter derfor løsningen.

Kripos støtter også den ordningen som foreslås for kundereskontro. Innholdet i den alminnelige kundereskontro er ikke av særlig personsensitiv karakter, og politiet bør således kunne få tilgang til opplysningene på lik linje med andre abonnementsopplysninger. Samtidig ser vi at utlevering av spesifiserte fakturaer, som tidvis kan inngå i en kundereskontro, har klare likhetstrekk med utlevering av ordinære trafikkdata. Den sontringen det legges opp til i lovforslaget, hvor tilgang til spesifiserte fakturaer fortsatt vil forutsette opphevelse av taushetsplikt, synes således fornuftig.

Med hilsen



Ketil Haukaas

Vedlegg

Saksbehandler:
Padv Håvar Undeland

Kopi:
Politidirektoratet
Det nasjonale statsadvokatembetet